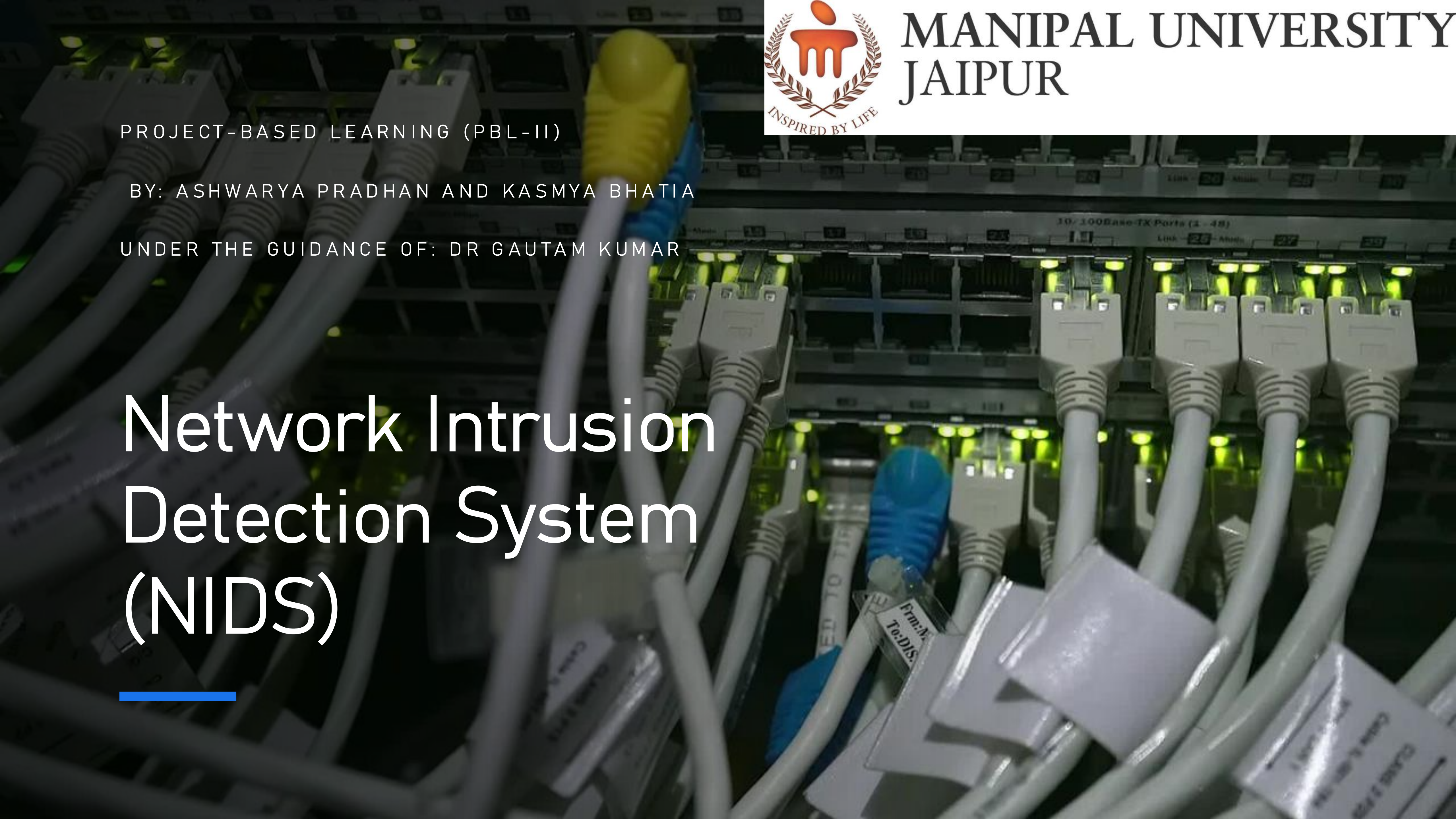


MANIPAL UNIVERSITY JAIPUR

PROJECT-BASED LEARNING (PBL-II)

BY: ASHWARYA PRADHAN AND KASMYA BHATIA

UNDER THE GUIDANCE OF: DR GAUTAM KUMAR

Network Intrusion Detection System (NIDS)

Introduction

- Cyber threats are constantly evolving, making it difficult for organizations to keep up. Traditional security measures such as firewalls and antivirus software can block known threats, but they are often ineffective against sophisticated cyber-attacks like malware infections, data breaches, and Denial-of-Service (DoS) attacks.
- A Network Intrusion Detection System (NIDS) plays a crucial role in cybersecurity by continuously monitoring network traffic in real-time to detect unauthorized activities and potential threats. By implementing a NIDS, organizations can strengthen their security posture and respond quickly to cyber incidents.

Objectives of NIDS

- Strengthen Network Security
- Improve Accuracy in Threat Detection
- Provide Instant Alerts and Quick Response
- Ensure Flexibility and Seamless Integration

Literature Survey

- Various NIDS solutions exist, each using different detection methods:
- Snort (Open-source IDS): Uses signature-based detection, highly customizable, but prone to false positives and ineffective against zero-day attacks.
- Suricata (High-performance IDS/IPS): Supports both signature and anomaly-based detection, optimized for high-speed networks but resource-intensive.
- Zeek (Network Monitoring Framework): Uses anomaly-based detection for unknown threats, provides detailed logging but requires advanced setup.
- Cisco Firepower (Commercial): AI-driven detection with high accuracy but costly and requires Cisco infrastructure.
- AWS GuardDuty (Cloud-based IDS): Automated, machine-learning-based detection, limited to AWS environments.

Comparative Study

System	Detection Type	Pros	Cons
Cisco Firepower	AI-driven (Machine Learning)	High accuracy, enterprise-grade protection	Expensive, requires Cisco infrastructure
AWS GuardDuty	Cloud-based IDS	Scalable, automated threat detection	Limited to AWS environments
Suricata	Hybrid (Signature + Anomaly)	High-speed, intrusion prevention capability	Resource-intensive for large deployments
Zeek	Anomaly-based	Effective for unknown threats, detailed logging	Complex setup, requires expertise
Snort	Signature-based	Open-source, customizable	High false positives, ineffective against zero-day attacks

Problem Definition & Requirements

- Cyber threats are becoming increasingly complex, and traditional security measures are insufficient. The main requirements for an advanced NIDS include:
- **Detecting various cyber threats**: DoS attacks, malware, unauthorized access.
- **Providing real-time monitoring and alerting**.
- **Minimizing false positives** using AI and ML techniques.
- **Ensuring scalability and integration** with existing security infrastructure.

System Design & Architecture

Packet Capture Module – Captures live network traffic and extracts relevant metadata.

Traffic Analysis Engine – Processes network packets and filters out normal traffic.

Threat Detection Model – Uses a combination of signature-based and anomaly-based detection.

Alert & Logging System – Generates alerts and stores log data for further analysis.

Implementation

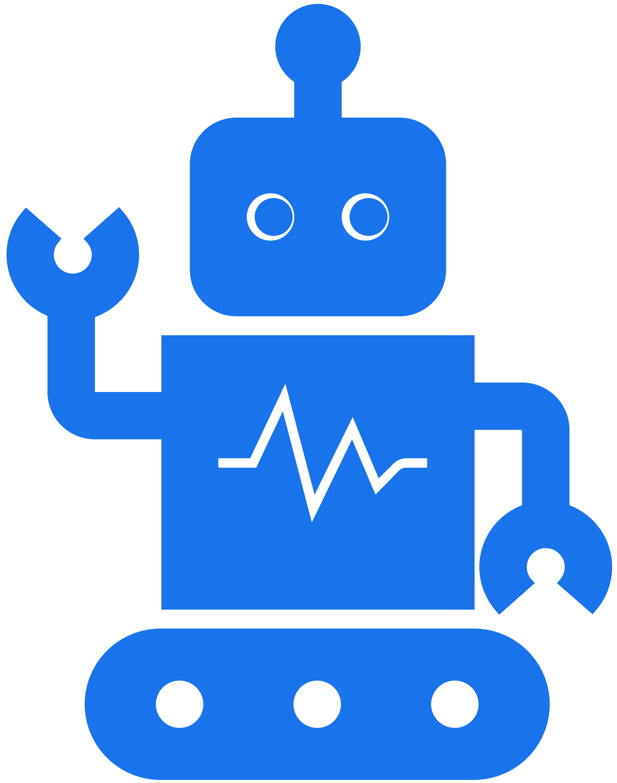
- **Programming Languages Used:** Python, C++
- **Tools and Libraries:** Wireshark, Scapy, Suricata, Snort
- **Database for Logging:** SQL/NoSQL
- **Visualization Dashboard:** Kibana/Grafana
- **Machine Learning for Threat Detection:** Uses AI models to detect patterns and minimize false positives.

Deployment & Scalability

- **On-Premises Deployment**: Installed on local servers for private networks.
- **Cloud Deployment**: Hosted on cloud platforms such as AWS, Azure.
- **Hybrid Implementation**: Combining on-premises and cloud-based monitoring for extended security.
- Scalability testing ensures the system handles increased network loads efficiently.

Future Enhancements

- To further improve the system, the following enhancements are planned:
- **AI-driven adaptive threat detection** to dynamically adjust threat patterns.
- **Automated incident response mechanisms** to take predefined actions against detected threats.
- **Mobile App Integration** for real-time security alerts.
- **Improved false positive reduction techniques** using advanced ML models.



References