PROJECT TOPIC: Intrusion Detection System Using Deep Learning

Group No.: 176

Project Group Members:

1. Deevyansh Chhabra (I-23/2115000331)
2. Shubham Goswami (I-64/2115000982)
3. Akshat Nogaraiya (H-5/2115000112)
4. Ashish Ojha (N-13/2115000222)
5. Vivek Kumar (M-67/2115001143)

Project Supervisor: Mr. Rahul Shandilya

About the Project: The project focuses on developing an Intrusion Detection System (IDS) that leverages deep learning (XLSTM) algorithms to identify and mitigate unauthorized access or malicious activities in a network. The IDS will analyse network traffic, identify patterns of normal behaviour, and flag anomalies indicating potential security breaches. The system will integrate real-time monitoring, anomaly detection, and an alert mechanism to enhance network security. By automating the detection process, the project aims to minimize manual intervention, reduce false positives, and improve response times in mitigating cyber threats. The use of deep learning (XLSTM) models enhances the accuracy of intrusion detection, ensuring proactive protection against emerging threats.

Motivation: With the rise in cyberattacks, the need for intelligent and automated intrusion detection systems is critical. Traditional IDS systems are often rule-based and prone to missing new and sophisticated attack vectors. This project utilizes deep learning (XLSTM) to address these gaps, making it an essential major project due to its relevance in addressing contemporary cybersecurity challenges. Its societal value lies in its potential to secure organizational networks, personal data, and critical infrastructure from evolving cyber threats**.**

Innovation:

1. **Real-Time Detection**: The system is capable of analysing network traffic in real time, allowing for immediate identification of threats.
2. **Deep learning (XLSTM)-Based Anomaly Detection**: Instead of rule-based systems, the project uses deep learning (XLSTM) algorithms that learn from network behaviour and detect previously unknown threats.
3. **Reduction of False Positives**: By incorporating advanced algorithms, the system reduces the number of false alerts, a common issue in traditional IDS systems.
4. **Self-Learning Capabilities**: The IDS can adapt and improve its detection accuracy as it is exposed to more data.
5. **Scalability**: The system is designed to scale across different network sizes, from small enterprises to large corporate environments.

6. **User-Friendly GUI**: A simple and intuitive graphical interface (Tkinter) will allow users to manage and monitor the system efficiently, even with limited technical expertise.

Project Planning:

Phase	Duration(Weeks)	Description
Research & Tool Learning	1	Learn about IDS, deep learning (XLSTM) models, and tools (Tkinter, Pytorch etc.)
Design & Planning	1	Design system architecture.
Dataset Preprocessing	1	Collect and preprocess the dataset for training the model.
Model Development and Training	2	Implement ML models and train them using the prepared dataset.
GUI Development	1	Create the user interface using Tkinter.
System Integration	1	Integrate the deep learning (XLSTM) models with the GUI and IDS system.
Testing & Evaluation	2	Test the system's accuracy performance, scalability,
Final Report Submission	1	Document the project and create presentation.

Tools required:

Hardware Requirements:

- Processor: Intel i5 or higher
- RAM: 8 GB (16 GB recommended)
- Storage: 500 GB SSD
- Network Adapters: Wi-Fi and Ethernet for network traffic analysis
- GPU (Optional, for faster ML model training)

Software Requirements:

- Operating System: Windows/Linux/macOS
- Python: Version 3.x
- Libraries: Scikit-learn, Pytorch (for advanced models), Pandas, NumPy, Tkinter (for GUI)
- IDE: PyCharm/VS Code/Jupyter
- Database: MySQL/SQLite (optional, if storing logs)
- Programming Language:

Signature of Project Supervisor: _____