# Multimodal Cyberattack Classification and Detection System

*Project Synopsis Submitted*

*to*

**MANIPAL ACADEMY OF HIGHER EDUCATION**

*For Partial Fulfillment of the Requirement for the*

*Award of the Degree*

*Of*

**Bachelor of Technology**

*in*

**Information Technology**

*by*

**Ishan Surana**

**Reg. No. 220911478**

*Under the guidance of*

Dr. Nisha P. Shetty
Assistant Professor - Senior Scale
Department of I&CT
Manipal Institute of Technology
Manipal, Karnataka, India

Dr. Raghevandra Ganiga
Assistant Professor - Senior Scale
Department of I&CT
Manipal Institute of Technology
Manipal, Karnataka, India


MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
*A Constituent Unit of MAHE, Manipal*

**October 2024**

**Objective:**

The objective of the "**Multimodal Cyberattack Detection and Classification System**" is to develop a robust solution for detecting and classifying cyberattacks. The system collects data from various devices and employs federated learning models for decentralized updates, ensuring data privacy. It integrates a hybrid cryptosystem for secure data transmission, utilizes blockchain for immutable result storage, and incorporates a feedback loop for continuous improvement and adaptability.

**Scope:**

This project encompasses the detection and classification of cyberattacks across multiple data modalities. It aims to enhance security through local data generation, federated learning, and blockchain integration, enabling efficient model updates while preserving user privacy and ensuring the integrity of the training process.

**Project Description:**

The system consists of four primary components:

1. **Multimodal Cyberattack Detection and Classification Model:**
    - **Local Data Generation:** Real-time data is collected directly from devices for model training and evaluation.
    - **Model Architecture:** A combination of deep learning architectures, including CNNs, RNNs, and Transformers, is utilized to analyze diverse cyberattack data. This includes feeding structural information and vectorized tokens into the neural network.
    - **Feature Fusion:** Features from various modalities are combined to create a comprehensive dataset for improved detection and classification.
2. **Federated Learning Framework:**
    - **Local Training:** Models are deployed on individual devices for local training using device-specific data.
    - **Update Aggregation:** Encrypted model updates (weights or gradients) are periodically sent to a central server.
    - **Privacy Preservation:** Techniques such as Secure Aggregation and Differential Privacy are employed to ensure raw data remains on the device.
3. **Blockchain Integration:**
    - **Result Storage:** Encrypted model updates and metadata are recorded on the blockchain for immutability and transparency.

- **Consensus Mechanism:** A consensus algorithm validates and reconciles model updates, maintaining a trustworthy global model.
- **Smart Contracts:** Smart contracts automate training schedules, update protocols, and compliance with security rules.

4. **Centralized Analysis and Coordination:**
    - **Global Model Refinement:** Updates from the blockchain are aggregated to enhance the central model.
    - **Result Analysis:** Aggregated results are analyzed to improve overall performance and accuracy.
    - **Feedback Distribution:** Updated model parameters are distributed back to devices for continuous improvement.

**Hardware Requirements:**

Processor: Intel dual core or above
Processor Speed: 1.0GHZ or above
RAM: 8 GB RAM or above
Hard Disk: 20 GB hard disk or above

**Software Requirements:**

- **Language:** Python
- **Frameworks:** TensorFlow, scikit-learn and transformers for ML model architecture
- **Blockchain**: Custom implementation of blockchain, deriving inspiration from Ethereum
- **Cryptosystem**: BB84 for secret exchange, coupled with AES for encryption. Secure communication protocols like HTTPS for data exchange

**Submitted by**


| Name | Registration number | Roll Number | Semester & Branch | Section |
|---|---|---|---|---|
| Ishan Surana | 220911478 | 39 | V (IT) [Batch 2] | A |
| Divej Ahuja | 220911482 | 40 | V (IT) [Batch 2] | A |
| Piyush Rangdal | 220911676 | 67 | V (IT) [Batch 2] | A |
| Udai Pratap Singh | 220911674 | 66 | V (IT) [Batch 2] | A |