## Lab 35 - Create a Threat Model for a Healthcare AI System

**Create a Threat Model for a Healthcare AI System**

**Lab Manual**



**Disclaimer: The content is curated from online/offline resources and used for educational purpose only**

**Task Description**

You will simulate a simple threat modeling scenario for a Healthcare AI system that predicts whether a patient has diabetes based on input data (like age, weight, sugar level).

We will simulate:

* Data input stage
* Risk assessment
* Simple STRIDE mapping

***Steps to create a Threat Model for a Healthcare AI System***

1. Visit the link: <https://colab.google/>
2. Click on ‘New Notebook’
3. Start typing the code given below
4. ***Installing the libraries***

# Required installations:

!pip install graphviz pandas matplotlib

1. ***Code to create a threat model and performing visualization***

# Required installations:

# pip install graphviz pandas matplotlib

from graphviz import Digraph

import pandas as pd

import matplotlib.pyplot as plt

from matplotlib.table import Table

from PIL import Image

# Step 1: Define ML pipeline

ml\_pipeline = {

    "Data Collection": "Patient health data (age, weight, sugar level)",

    "Preprocessing": "Cleaning and normalizing data",

    "Model Training": "Train decision tree model",

    "Deployment": "Web API for predictions",

    "Inference": "User inputs -> predictions"

}

# Step 2: STRIDE threats with color codes

stride\_threats = {

    "Spoofing": {

        "Example": "Fake patient ID to access system",

        "Color": "#FFC0CB"  # Light pink

    },

    "Tampering": {

        "Example": "Changing training data to mislead predictions",

        "Color": "#FFA07A"  # Light salmon

    },

    "Repudiation": {

        "Example": "No logs to trace incorrect prediction",

        "Color": "#FFFF99"  # Light yellow

    },

    "Information Disclosure": {

        "Example": "Leaking patient medical history",

        "Color": "#ADD8E6"  # Light blue

    },

    "Denial of Service": {

        "Example": "Sending too many requests to crash system",

        "Color": "#D3D3D3"  # Light grey

    },

    "Elevation of Privilege": {

        "Example": "Nurse accessing doctor-level permissions",

        "Color": "#90EE90"  # Light green

    }

}

# Step 3: Visualize ML Pipeline using Graphviz

dot = Digraph(comment='ML Pipeline for Healthcare')

dot.attr(rankdir='LR', size='10,5')

for stage, asset in ml\_pipeline.items():

    dot.node(stage, f"{stage}\n{asset}", shape='box', style='filled', fillcolor='lightblue')

stages = list(ml\_pipeline.keys())

for i in range(len(stages) - 1):

    dot.edge(stages[i], stages[i + 1])

# Render and show the pipeline image

dot.render('ml\_pipeline', format='png', cleanup=False)

Image.open('ml\_pipeline.png').show()

# Step 4: Visualize STRIDE threats with color-coding using matplotlib

fig, ax = plt.subplots(figsize=(11, 3))

ax.set\_axis\_off()

table = Table(ax, bbox=[0, 0, 1, 1])

# Table column headers

columns = ["STRIDE Threat", "Example"]

n\_rows = len(stride\_threats)

n\_cols = len(columns)

widths = [0.2, 0.8]

# Add table headers

for col\_index, column in enumerate(columns):

    cell = table.add\_cell(0, col\_index, widths[col\_index], 0.2, text=column, loc='center', facecolor='lightgray')

    cell.get\_text().set\_fontweight('bold')

# Add table rows

for row\_index, (threat, details) in enumerate(stride\_threats.items(), start=1):

    table.add\_cell(row\_index, 0, widths[0], 0.2, text=threat, loc='left', facecolor=details["Color"])

    table.add\_cell(row\_index, 1, widths[1], 0.2, text=details["Example"], loc='left', facecolor=details["Color"])

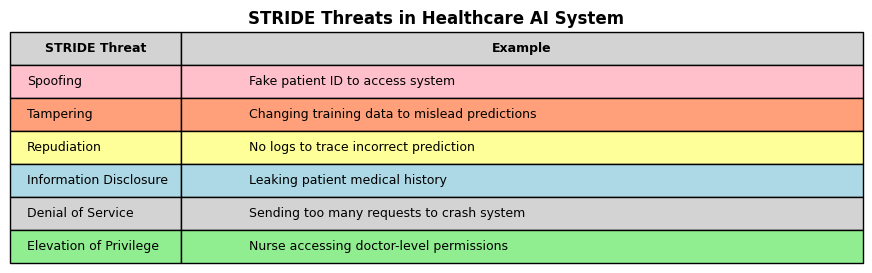
ax.add\_table(table)

plt.title("STRIDE Threats in Healthcare AI System", fontweight='bold')

plt.show()

1. Now click on ***Run All*** or ***Ctrl + F9*** to run all the cells

**Output:**

****

**Explanation**

| **STRIDE Threat** | **What it Means** | **Example in the Table** | **Color** |
| --- | --- | --- | --- |
| **Spoofing** | Someone **pretends to be someone else** to trick the system. | Fake patient ID to access system | Light Pink |
| **Tampering** | **Changing data or code** so that the system behaves wrongly. | Changing training data to mislead predictions | Light Orange |
| **Repudiation** | **No proof or logs** of who did what, so no one can be held accountable. | No logs to trace incorrect prediction | Light Yellow |
| **Information Disclosure** | **Leaking private information** to the wrong person. | Leaking patient medical history | Light Blue |
| **Denial of Service** | **Flooding the system** with requests so that it **crashes or becomes very slow**. | Sending too many requests to crash system | Light Grey |
| **Elevation of Privilege** | Someone **gets more access** than they are allowed — like breaking into admin or doctor features. | Nurse accessing doctor-level permissions | Light Green |

This visual helps you:

* **Understand security risks** in a healthcare AI system.
* **Relate each threat to a real-world example**.
* **Visually separate threats** using colors.