**Objective:**

The primary objective of this research is to evaluate the vulnerability of sensitive medical information transmitted between two Raspberry Pi devices. This involves conducting three common cyberattacks - Man-in-the-Middle, Replay, and DDoS - to assess the potential risks and vulnerabilities. Additionally, the research aims to develop and implement a detection and prevention system to mitigate these threats and protect the sensitive data.

**Scope:**

The scope of this research encompasses:

* Establishing a secure communication channel between two Raspberry Pi devices for transmitting medical information.
* Implementing three common cyberattacks (Man-in-the-Middle, Replay, and DDoS) to assess the vulnerability of the communication channel.
* Developing and implementing a detection and prevention system to identify and mitigate the aforementioned attacks.
* Analyzing the effectiveness of the detection and prevention system in protecting sensitive medical information.

**Need for the Application:**

The need to protect sensitive medical information is paramount in today's healthcare landscape. Breaches of medical records can lead to severe consequences, including identity theft, financial loss, and damage to patient trust. This research is essential to understand the vulnerabilities and develop effective security measures to safeguard sensitive medical data transmitted between devices.

**Project Description:**

**Problem Statement:**

The transmission of sensitive medical information between devices poses significant security risks due to the potential for interception, tampering, and unauthorized access. This research aims to address these vulnerabilities and develop robust security measures to protect such data.

**Functionalities to be Implemented:**

1. Secure Communication Channel: Establish a secure communication channel between two Raspberry Pi devices using encryption protocols (e.g., TLS, HTTPS) to protect data in transit.
2. Attack Simulation: Implement the Man-in-the-Middle, Replay, and DDoS attacks to simulate real-world threats and assess their impact on the communication channel.
3. Detection and Prevention System: Develop a system capable of detecting anomalies and signs of attacks, such as unusual traffic patterns, unauthorized access attempts, or data integrity violations. Implement preventive measures like intrusion detection systems, firewalls, and encryption to mitigate these threats.
4. Data Analysis: Collect and analyze data from the attacks and the detection and prevention system to evaluate the effectiveness of the security measures and identify areas for improvement.

By addressing these functionalities, this research will provide valuable insights into the vulnerabilities of medical data transmission and offer practical solutions for enhancing its security.

**Hardware Requirements:**

2 Raspberry Pi Devices, Network Interface, Cables, Laptop, Power Supply

**Software Requirements:**

Raspberry Pi OS, OpenSSL, scapy, hping3, Wireshark, Snort, iptables, fail2ban

**Submitted by**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Registration number | Roll Number | Semester & Branch | Section |
| Eva Hemantkumar Shah | 220911668 | 65 | V (IT) | C |
| Arnav Aradhya | 220911612 | 56 | V (IT) | C |
| Yashaswini Pinnaka | 220911662 | 64 | V (IT) | C |