CYBERSECURITY TRACK

Problem Statement: Securing USB Data Transfer

Background:

USB devices are commonly used for data transfer between computers and various peripherals. However, these devices pose security risks due to the potential introduction of malware or unauthorized data access. Ensuring the integrity and confidentiality of data transferred via USB is crucial for cybersecurity.

Challenge:

Develop a simple and cost-effective hardware solution to enhance the security of USB data transfer. The solution should address one or more of the following aspects:

Malware Detection: Create a mechanism to detect and prevent the transfer of malware from USB devices to the connected computer. The solution should automatically scan USB devices for potential threats before allowing data transfer.
Data Encryption: Implement a straightforward encryption method to secure the data transferred via USB. The encryption should be applied in real-time during data transfer, ensuring that even if unauthorized access occurs, the data remains confidential.
Access Control: Design a basic access control system that allows users to specify which USB devices are permitted to connect to their computers. This feature should prevent unauthorized USB devices from initiating data transfer.
User-Friendly Interface: Develop a user-friendly interface that enables easy setup and management of the security features. Consider the needs of users with varying levels of technical expertise.
Compatibility: Ensure that the solution is compatible with commonly used operating systems and does not disrupt the normal functionality of USB devices. The hardware should be plug-and-play, requiring minimal configuration.

Expected Impact:

A successful solution to this challenge will provide an accessible and effective way to enhance USB data transfer security, particularly for users who may not have advanced cybersecurity knowledge. The solution should be straightforward to implement and seamlessly integrate into existing computing environments.

Evaluation Criteria:

Participants will be evaluated based on the simplicity, effectiveness, and usability of their hardware solution. Consideration will be given to the clarity of the user interface, the efficiency of malware detection, and the overall feasibility of the proposed security features.