FINAL ASSIGNMENT

Bùi Thành Long – 20205160

5 RISKS is:

1. Insecure Communication:

Risk: IoT devices often communicate over networks, and if the communication channels are not properly secured, it opens the door to eavesdropping and data tampering.

Solution: Implement strong encryption protocols (e.g., TLS/SSL) for data in transit. Use secure communication channels and regularly update cryptographic protocols to address emerging vulnerabilities.

2. Weak Authentication and Authorization:

Risk: Inadequate authentication and authorization mechanisms can lead to unauthorized access to IoT devices, allowing malicious actors to control or manipulate connected devices.

Solution: Implement robust authentication methods, such as two-factor authentication (2FA) and strong password policies. Employ access controls and ensure that each device and user has appropriate permissions.

3. Device Vulnerabilities and Lack of Updates:

Risk: Many IoT devices have limited processing capabilities, making it challenging to implement strong security measures. Additionally, manufacturers may not release timely security updates, leaving devices vulnerable to exploitation.

Solution: Regularly update and patch firmware to address security vulnerabilities. Employ secure coding practices during device development and design devices with over-the-air (OTA) update capabilities for easy and prompt updates.

4. Insufficient Data Protection:

Risk: IoT devices often collect and process sensitive data. If this data is not adequately protected, it can lead to privacy breaches and misuse of personal information.

Solution: Employ end-to-end encryption to protect data both in transit and at rest. Implement secure storage practices on devices, and minimize the collection of unnecessary sensitive data to reduce the potential impact of a breach.

5. Lack of Physical Security:

Risk: Physical access to IoT devices can lead to unauthorized manipulation, tampering, or theft of devices, potentially compromising the entire system.

Solution: Implement physical security measures, such as tamper-evident packaging and secure installation locations. Ensure that devices have mechanisms to detect and respond to physical tampering, such as disabling functionality or triggering alarms.