

Universidad de Guadalajara

Centro Universitario de Ciencias exactas e
Ingenierías



Ingeniería en computación

SEGURIDAD D04

Actividad 5.3 Problemática de seguridad en Internet de las cosas

Profesora: ARMIDA GRISELDA VAZQUEZ CURIEL

Integrantes:

Gildo López Miguel Ángel

González Ramírez Alan Leonardo

Montejano Paredes Diego Fernando

Pérez Juárez Juan Antonio

Fecha: 29/04/2024

Índice

Portada	1
Objetivo	2
Introducción	2
Contenido	2
Desarrollo del proyecto	3
1. Datos con Arduino	3
2. Diseño de la Base de Datos	4
3. Visualización de Datos con Python	5
Conclusión	6
Bibliografía	7

Objetivo

Realizar un dispositivo IoT por ejemplo con Arduino e identificar sus fallas de seguridad (hacer un reporte al respecto).

Introducción

La seguridad de los dispositivos IoT es un tema importante en la actualidad, ya que estos dispositivos están cada vez más presentes en nuestra vida cotidiana. La interconectividad y el acceso remoto que ofrecen estos dispositivos pueden facilitar la vida de los usuarios, pero también pueden crear oportunidades para los malos actores que buscan robar datos privados. Para proteger tus dispositivos IoT, es importante seguir buenas prácticas de seguridad, como asegurarse de que se proporcionen actualizaciones y aplicarlas de manera consistente cada vez que estén disponibles. En este proyecto, se utilizará Arduino para detectar la temperatura cada X segundos y enviarla a la computadora. Para ello, se programará un sensor de temperatura para que detecte la temperatura y se enviará la información a través del puerto serie de Arduino. El

tiempo de espera entre lecturas se puede ajustar cambiando el valor de la variable intervalo.

Contenido

La implementación de un sistema IoT, como en nuestro proyecto de monitorización de temperatura en un invernadero, introduce desafíos específicos de seguridad que requieren una atención especial. A continuación, se destacan algunas consideraciones clave en el ámbito de la seguridad del IoT:

1. **Dispositivos Conectados:** Los dispositivos IoT, como nuestro sensor de temperatura Arduino, están interconectados, lo que aumenta la superficie de ataque potencial. Es crucial implementar prácticas de seguridad sólidas en la autenticación y autorización de dispositivos. Se deben utilizar estándares de cifrado robustos para proteger la comunicación entre dispositivos y la central.
2. **Privacidad de los Datos:** La información recopilada por los dispositivos IoT puede ser altamente sensible. La seguridad en el manejo de datos debe incluir medidas para preservar la privacidad de los usuarios y garantizar que solo las partes autorizadas tengan

acceso a información específica. En nuestro caso, la temperatura del invernadero puede considerarse información confidencial, y su acceso debe limitarse de manera adecuada.

3. **Actualizaciones de Firmware:** Los dispositivos IoT deben contar con mecanismos eficientes para la actualización de firmware. La capacidad de corregir vulnerabilidades de seguridad y actualizar la funcionalidad es esencial para garantizar la resistencia continua contra amenazas emergentes. Los desarrolladores deben diseñar estos procesos de actualización de manera que sean seguros y no propicien la introducción de malware o manipulación no autorizada.
4. **Gestión de Identidad y Acceso:** La gestión efectiva de la identidad y el acceso es crítica. Los sistemas deben autenticar de manera segura a los usuarios y dispositivos, y se deben aplicar principios de mínimos privilegios para limitar el acceso solo a lo necesario. La implementación de protocolos como OAuth y OpenID Connect puede mejorar la seguridad en la gestión de identidad.
5. **Análisis de Riesgos Continuo:** Dada la evolución constante de las amenazas, es esencial realizar un análisis de riesgos continuo. Los equipos de desarrollo deben estar al tanto de las amenazas emergentes y adaptar las medidas de seguridad en consecuencia. La colaboración con la comunidad de seguridad y la participación en programas de divulgación de vulnerabilidades pueden ser estrategias efectivas.
6. **Integración de Estándares de Seguridad:** La adopción de estándares de seguridad reconocidos, como el conjunto de directrices del NIST (National Institute of Standards and Technology) o ISO/IEC 27001, puede proporcionar una base sólida para el diseño y la implementación segura de sistemas IoT.

Desarrollo del proyecto

A medida que abordamos esta iniciativa, no solo nos enfocamos en la funcionalidad y eficiencia del sistema, sino que también ponemos un énfasis significativo en la seguridad de la información. El proyecto se desglosa en tres componentes principales, cada uno de los cuales se diseña y evalúa considerando las posibles amenazas y vulnerabilidades:

1. Datos con Arduino

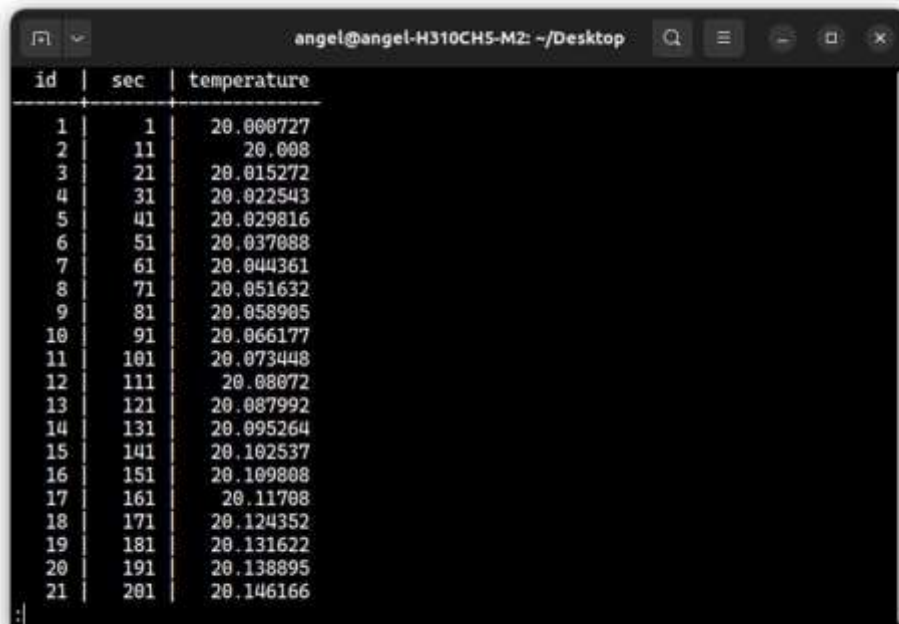
Para la adquisición de datos, se desarrollará un programa específico para Arduino. Este programa se encargará de medir la temperatura a intervalos definidos, permitiendo que el usuario ajuste estos intervalos a través de la interfaz de Arduino IDE.

Dado que la captura de datos en el entorno físico puede exponer los dispositivos a riesgos, nos enfocaremos en implementar medidas de seguridad. Se explorarán y aplicarán métodos de cifrado y autenticación para prevenir posibles ataques de manipulación de datos o accesos no autorizados durante la transmisión de datos a la computadora central.

2. Diseño de la Base de Datos

La seguridad de la base de datos es fundamental, ya que almacenará información sensible sobre las condiciones ambientales del invernadero. El diseño de la base de datos contemplará mecanismos de control de acceso robustos para limitar el acceso a usuarios autorizados. Además, se evaluará la resistencia de la base de datos frente a posibles intentos de intrusión, implementando

medidas preventivas para garantizar su integridad. Se considerarán estrategias de respaldo y recuperación para preservar la continuidad de los datos en caso de incidentes de seguridad.



A terminal window titled 'angel@angel-H310CH5-M2: ~/Desktop' displays a table with three columns: 'id', 'sec', and 'temperature'. The table contains 21 rows of data, showing a steady increase in both 'id' and 'sec' values, while 'temperature' values fluctuate slightly around 20.0.

id	sec	temperature
1	1	20.000727
2	11	20.0008
3	21	20.015272
4	31	20.022543
5	41	20.029816
6	51	20.037088
7	61	20.044361
8	71	20.051632
9	81	20.058905
10	91	20.066177
11	101	20.073448
12	111	20.08072
13	121	20.087992
14	131	20.095264
15	141	20.102537
16	151	20.109808
17	161	20.11708
18	171	20.124352
19	181	20.131622
20	191	20.138895
21	201	20.146166



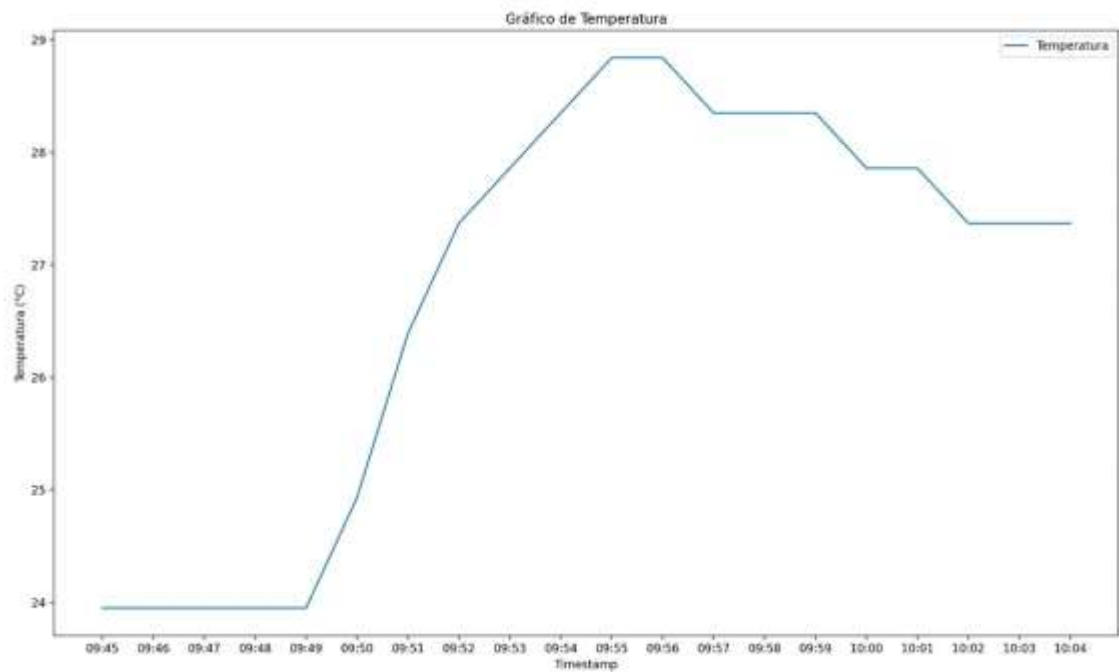
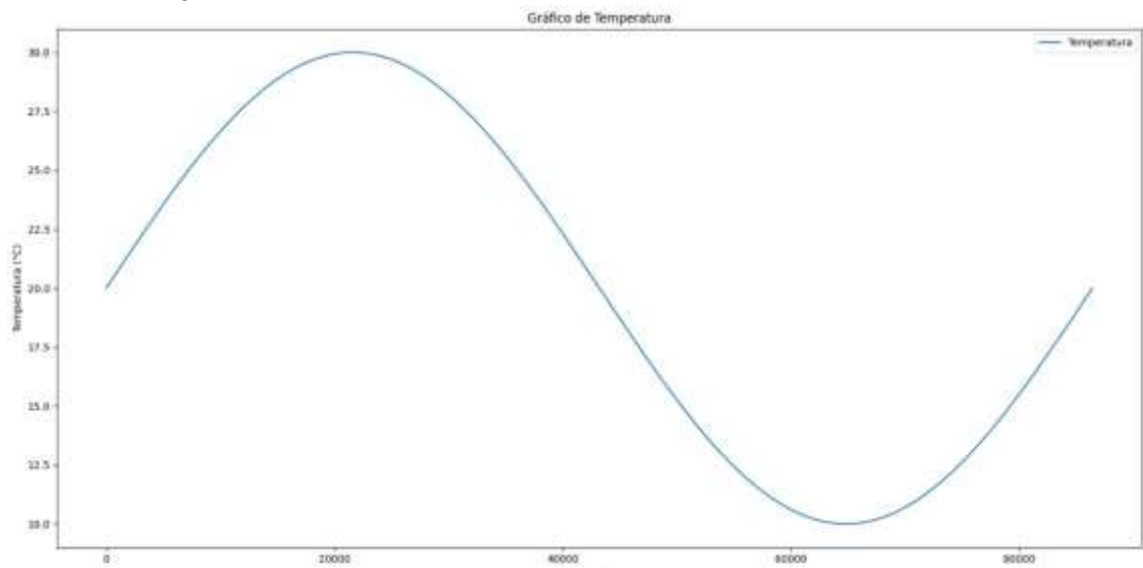
A terminal window displays a series of temperature readings over time. Each line shows the current time (Hora) and the corresponding temperature (Temperatura). The temperature starts at 23.95 and rises to 28.84 by 10:09:56, then fluctuates between 27.37 and 28.35 until 10:10:04.

```
Hora: 10:09:45, Temperatura: 23.95
Hora: 10:09:46, Temperatura: 23.95
Hora: 10:09:47, Temperatura: 23.95
Hora: 10:09:48, Temperatura: 23.95
Hora: 10:09:49, Temperatura: 23.95
Hora: 10:09:50, Temperatura: 24.93
Hora: 10:09:51, Temperatura: 26.39
Hora: 10:09:52, Temperatura: 27.37
Hora: 10:09:53, Temperatura: 27.86
Hora: 10:09:54, Temperatura: 28.35
Hora: 10:09:55, Temperatura: 28.84
Hora: 10:09:56, Temperatura: 28.84
Hora: 10:09:57, Temperatura: 28.35
Hora: 10:09:58, Temperatura: 28.35
Hora: 10:09:59, Temperatura: 28.35
Hora: 10:10:00, Temperatura: 27.86
Hora: 10:10:01, Temperatura: 27.86
Hora: 10:10:02, Temperatura: 27.37
Hora: 10:10:03, Temperatura: 27.37
Hora: 10:10:04, Temperatura: 27.37
```

3. Visualización de Datos con Python

La fase de visualización de datos se abordará mediante una aplicación en Python. Esta aplicación se conectará a la base de datos, recuperará los datos almacenados y los presentará en una interfaz gráfica.

La seguridad será una preocupación clave en esta etapa; se examinarán y aplicarán prácticas de programación segura para evitar vulnerabilidades comunes, como inyecciones de código. La implementación de medidas de autenticación y autorización garantizará que solo usuarios autorizados tengan acceso a la información visualizada.



Conclusión

En la adquisición de datos con Arduino, se reconoce la importancia de la seguridad en la captura y transmisión de datos. La implementación de métodos de cifrado y autenticación proporciona una capa sólida de protección contra manipulaciones y accesos no autorizados. No obstante, la necesidad de una mayor exploración de medidas de seguridad para el dispositivo Arduino, considerando escenarios en los que el acceso al entorno del invernadero pueda representar una amenaza.

El diseño de la base de datos para almacenar la información del invernadero ha sido una tarea desafiante pero crucial. La implementación de mecanismos de control de acceso robustos es esencial para salvaguardar la confidencialidad de los datos. Sin embargo, se podría mejorar la resistencia de la base de datos mediante la exploración de técnicas avanzadas de encriptación y la implementación de análisis de vulnerabilidades más detallados. Además, la consideración de estrategias de respaldo y recuperación ha sido fundamental, pero podría beneficiarse de una evaluación más profunda.

La implementación de prácticas seguras de programación ha sido central para prevenir vulnerabilidades comunes. Sin embargo, reconozco la necesidad de una mayor integración de medidas de autenticación y autorización en la aplicación para reforzar aún más la seguridad del sistema. La colaboración continua con los demás miembros del equipo en este aspecto y la actualización regular de las prácticas de seguridad serán esenciales para mantener la robustez de la aplicación en el tiempo.

Bibliografía

Del Valle Hernández, L. (2021, March 23). Leer el sensor de temperatura LM35 en

Arduino. Programarfacil Arduino y Home Assistant.

<https://programarfacil.com/blog/arduino-blog/leer-el-sensor-de-temperaturalm35-en-arduino/>

Fisher, S. (2023, February 24). Riesgos de seguridad en el Internet de las cosas. Riesgos

De Seguridad En El Internet De Las Cosas. <https://www.avast.com/es-es/c-iotsecurity-risks>

Ramírez, H. (2023, August 9). Seguridad en el internet de las cosas (IoT): Qué es, riesgos

y cómo protegernos. Grupo Atico34. <https://protecciondatos-lopd.com/empresas/seguridad-internet-de-las-cosas/>