espol Facultad de Ingeniería en Electricidad y Computación

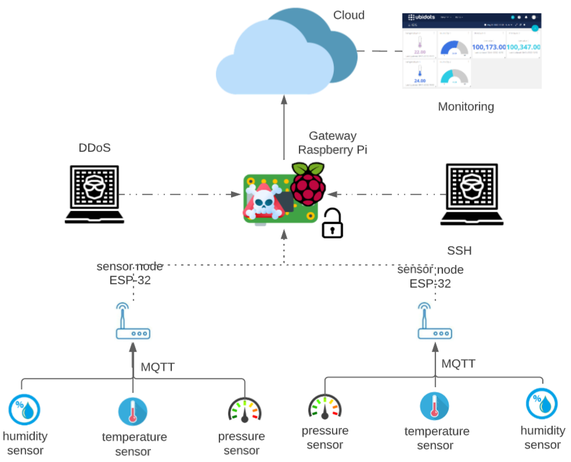
Genessis M. Enriquez
gemaenri@espol.edu.ec

Cristopher D. Vega
cdvega@espol.edu.ec

Desarrollo de un sistema inteligente de detección de Intrusos en una infraestructura IoT para agricultura de precisión

PROBLEMA

Los dispositivos IoT (*Internet of Things*) utilizados en agricultura de precisión no son seguros, debido a que son vulnerables a ataques. Ante ello, es necesario desarrollar un sistema que detecte y alerte anomalías de red para evitar el robo o perdida de datos.



OBJETIVO GENERAL

Desarrollar un sistema inteligente de detección de intrusos y anomalías usando machine learning para el mejoramiento de la seguridad de una infraestructura IoT orientada a la agricultura de precisión.

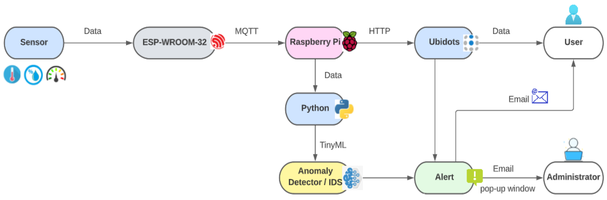
PROPUESTA

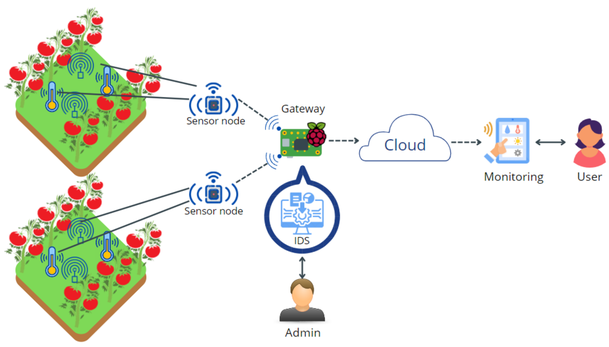
El proyecto se enfoca en el desarrollo de un IDS (*Intrusion Detection System*) inteligente usando TinyML, proporcionando un sistema capaz de detectar, reaccionar y alertar ataques para brindar mayor seguridad a la infraestructura IoT.

Esta solución puede ser aplicada en agricultura de precisión para dar seguridad a los datos de los sensores, los cuales sirven para el monitoreo de diversos productos, tales como tomates, banano, cacao.

Se creó una infraestructura IoT en los alrededores del Laboratorio de Sistemas Telemáticos para simular un área de agricultura con el fin de obtener datos reales y de detectar anomalías.

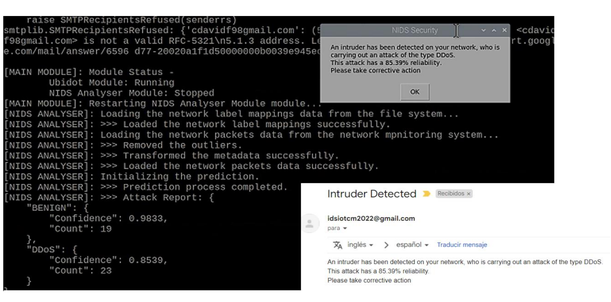
Para entrenar el IDS inteligente se usan datos del tráfico de red de la Raspberry Pi. Adicionalmente, se realizan dos tipos de ataques DDoS y fuerza bruta por medio de SSH. Se sostiene una condición ideal de que el atacante se encuentra dentro de la misma red que la Raspberry Pi. Con ello, se hace una comparación del sistema, del antes y después de ejecutar el IDS.

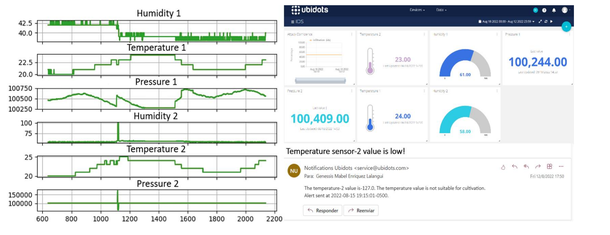




RESULTADOS

- Los datos de los sensores son enviados a los nodos y estos envían esta información a la Raspberry Pi usando MQTT por medio de Wi-Fi. Luego, desde la Raspberry son subidos a Ubidots para el monitoreo.
- Se envía un correo con una notificación/alerta al usuario al detectar anomalías en los valores de los sensores cuando el valor está fuera del rango adecuado para el cultivo de tomates. Por ejemplo, para la temperatura el rango es entre 18°C y 28°C, para la humedad es de 34% y a 70% y la presión debe estar alrededor de los 1000 hPa.
- El IDS al detectar un ataque DDoS muestra una ventana emergente alertando al administrador del ataque con el porcentaje de fiabilidad de la detección y envía un correo alertando el tipo de ataque del que fue víctima.
- El sistema de la Raspberry Pi se ralentiza cuando es atacado con o sin el IDS. Por este motivo se pierde un 66,67% de datos en ambos casos.





CONCLUSIONES

- El tiempo del análisis de predicción del sistema de detección inteligente fue de 1 segundo con 6 milisegundos. Este tiempo puede disminuir si se sigue con el entrenamiento del IDS con una mayor frecuencia de ataques. El fin es que aumente la precisión y el tiempo de detección de los ataques sea más rápido.
- El IDS mostró una fiabilidad del 85.39% al momento de detectar intrusos en la Raspberry Pi durante los ataques. Esto demuestra una gran eficiencia del sistema.
- Se tuvo un promedio de error del 2.8% en la predicción de los datos que corresponden a los sensores que funcionan correctamente y para el caso de sensores con una anomalía el porcentaje de error ascendió al 41.7%. Lo que coincide con la detección y notificación del detector de anomalías.
- Antes del IDS un intruso podía realizar un ataque sin ser detectado. Con la ejecución del IDS, el programa notificó/alertó el ataque al administrador, evitando el robo o perdida de información. Esto mejoró la seguridad, aumentando la confiabilidad de los dispositivos.