Universidad CENFOTEC
Maestría Profesional en Ciberseguridad
Escuela de Ciberseguridad

Tema:

"Propuesta de un sistema de monitoreo y detección de eventos de seguridad para tráfico de red en dispositivos IoT residenciales utilizando una arquitectura cloud en AWS"

Elaborado por:
Oscar Arias Quesada

Abril 2026

Declaratoria de derechos de autor

Yo, Oscar Eduardo Arias Quesada, en mi condición de autor del presente trabajo de investigación, presentado como requisito para optar por el grado de Maestría en Ciberseguridad en la Universidad CENFOTEC, declaro bajo fe de juramento que la autoría de este documento me pertenece en su totalidad. Por consiguiente, las ideas, doctrinas, resultados y conclusiones expuestas en esta obra son de mi exclusiva responsabilidad.

Asimismo, se autoriza el uso y consulta de este estudio con fines estrictamente académicos y de investigación. Se prohíbe de forma expresa cualquier reproducción total o parcial, así como el uso no autorizado de la tesis para fines de comercialización o lucro.

Propuesta de un sistema de monitoreo y detección de eventos de seguridad para tráfico de red en dispositivos IoT residenciales utilizando una arquitectura cloud en AWS

Abstract

En el contexto residencial actual, el crecimiento exponencial de dispositivos IoT ha multiplicado los vectores de ataque sobre las redes domésticas, exponiendo datos sensibles y recursos críticos a amenazas persistentes. Frente a esta realidad, la presente tesis propone un sistema integral de monitoreo y detección de eventos de seguridad centrado en el análisis de tráfico de red generado por dispositivos IoT residenciales. Utilizando servicios de AWS para ingestión de datos, se diseña una canalización escalable que captura, analiza y verifica flujos de red, permitiendo la identificación temprana de patrones anómalos mediante una serie de reglas predefinidas.

La propuesta contempla un módulo de gestión centralizada que analiza alertas, además de un sistema de notificaciones automatizadas ante incidentes críticos. El enfoque combina criterios de desempeño, costo y cumplimiento de buenas prácticas de seguridad en la nube, garantizando alta disponibilidad y tolerancia a fallos. Se valida la eficacia del sistema mediante pruebas de intrusión simuladas y escenarios de ataque reales, demostrando una postura de defensa proactiva en entornos domésticos inteligentes.

Palabras Clave: IoT, monitoreo, tráfico de red, cloud, AWS.

1. Introducción

El incremento exponencial en la adopción de dispositivos del Internet de las Cosas (IoT) en los hogares costarricenses ha transformado la dinámica cotidiana hacia entornos más automatizados y eficientes; no obstante, esta integración tecnológica ha ocurrido de manera más acelerada que la implementación de medidas de protección adecuadas, convirtiendo a las redes domésticas en un objetivo primario para la ciberdelincuencia. La naturaleza de estos dispositivos, diseñados frecuentemente priorizando la funcionalidad sobre la seguridad, ha expandido críticamente la superficie de ataque en el ecosistema digital residencial, donde el histórico de estas tecnologías revela debilidades estructurales como la falta de cifrado

en las comunicaciones, mecanismos de autenticación deficientes y la omisión de actualizaciones regulares de software. Estos factores permiten que actores maliciosos exploten los nodos no solo para extraer información sensible, sino para utilizarlos como plataformas de ataque hacia otros sistemas, dejando en evidencia que la protección actual sigue siendo inconsistente y carece de un enfoque técnico especializado.

Esta problemática se agrava en el contexto nacional, donde la penetración del Internet de banda ancha alcanza a la gran mayoría de las viviendas, superando drásticamente la capacidad de defensa de las arquitecturas de red convencionales. Los enrutadores residenciales estándar, al actuar como infraestructura crítica de conectividad, presentan una superficie de ataque significativa debido a la obsolescencia en su firmware y debilidades en sus protocolos, pero fundamentalmente porque carecen de la potencia de cómputo necesaria para ejecutar tareas de seguridad avanzada. Esta carencia sistemática de mecanismos de defensa nativos facilita que los dispositivos sean reclutados en redes de bots o sirvan como vectores para el movimiento lateral dentro de la red interna, donde los firewalls domésticos tradicionales resultan ineficaces al depender de firmas estáticas y carecer de memoria para el análisis histórico del tráfico.

Ante este escenario, se vuelve imperativo el desarrollo de un sistema de monitoreo y detección de eventos de seguridad implementado sobre una arquitectura cloud en Amazon Web Services (AWS). Esta propuesta se justifica por la persistente falta de visibilidad en las redes domésticas y la capacidad de la nube para superar las limitaciones de procesamiento locales mediante herramientas como AWS IoT Core. A diferencia de los dispositivos de red tradicionales, un enfoque basado en la nube permite la implementación de modelos para la detección de anomalías comportamentales en tiempo real, identificando desviaciones en los patrones de tráfico como escaneos masivos, exfiltración de datos o servicios sin cifrado. Al integrar este monitoreo, no solo se reduce el tiempo de detección de incidentes, sino que se habilita una respuesta técnica reproducible y auditable que garantiza un nivel de protección robusto para el tráfico de red en los entornos domésticos conectados.

2. Método

La investigación adoptó una metodología mixta que combina el análisis cualitativo y cuantitativo para recolectar información detallada sobre los patrones de ciberataques y la eficacia de las medidas de protección. Este enfoque permitió no solo obtener datos numéricos sobre la frecuencia de las amenazas, sino también comprender las características subyacentes de las vulnerabilidades en los dispositivos IoT mediante la revisión de literatura especializada y casos de estudio previos.

Fase de Diagnóstico e Infraestructura de Prueba

Para la captura y análisis del tráfico, se diseñó una infraestructura de red residencial controlada, compuesta por un enrutador principal y un punto de acceso (AP) configurado en una computadora con Windows 10 bajo la función de "Zona de cobertura inalámbrica móvil". Este diseño permitió que todo el tráfico de los dispositivos IoT fluyera a través del gateway local, facilitando la captura de paquetes mediante herramientas como Wireshark. Se seleccionaron tres categorías de dispositivos para representar el ecosistema común de un hogar inteligente: Cámara IP: Dispositivo de video vigilancia que genera flujos densos de datos UDP. Bombillo Inteligente: Nodo de baja potencia que utiliza protocolos de mensajería ligera. Tomacorriente Inteligente: Dispositivo de gestión de energía que permite analizar patrones de conexión y estados de encendido/apagado.

Implementación del Módulo de Captura y Preprocesamiento

El sistema utiliza un gateway local que ejecuta un script de Python optimizado con la biblioteca Scapy para realizar la recolección y anonimización del tráfico de red residencial. El proceso de preprocesamiento ligero es vital para garantizar la eficiencia del ancho de banda y la privacidad del usuario, ya que el sistema no envía el contenido de los paquetes (payload) a la nube, sino únicamente metadatos estructurados en formato JSON.

Herramientas de Análisis de Tráfico en el Gateway	Función en el Sistema
Wireshark	Captura de trazas PCAP en tiempo real
Python / Scapy	Transformación de trazas a métricas JSON y filtrado de protocolos
MQTT (Protocolo)	Publicación segura de mensajes hacia AWS IoT Core
Kali Linux	Simulación de escenarios de ataque para validación

La estrategia de desarrollo incluyó la consolidación de datos bajo un modelo "3-a-1", donde las métricas de múltiples dispositivos se agrupan en un único mensaje de reporte enviado a AWS cada 60 segundos. Esto no solo reduce la carga en la red, sino que minimiza los costos de ingestión de datos en la plataforma cloud.
Para propósitos de la validación experimental, se utilizó un esquema simplificado de un único certificado compartido para el Gateway, definiéndose la migración hacia identidades criptográficas individuales (X.509 por dispositivo) como un requisito indispensable para despliegues reales fuera del laboratorio.

Diseño de la Arquitectura Cloud en AWS

La inteligencia del sistema reside en AWS, configurada mediante una canalización de datos escalable que integra los siguientes servicios nativos:

- **AWS IoT Core**: Gestiona la conexión segura de los dispositivos (Things) mediante autenticación mutua con certificados X.509 y cifrado TLS.
- **AWS Lambda**: Actúa como el motor de toma de decisiones, analizando las métricas de red para identificar escaneos ARP, ataques de fuerza bruta o conexiones desde direcciones IP no autorizadas.
- **AWS CloudWatch**: Almacena los logs de eventos para análisis forense y auditoría histórica de los comportamientos de red.

- **Amazon SNS**: Orquesta las notificaciones automáticas hacia el usuario final ante incidentes críticos de seguridad.

3. Resultados

Los resultados de la investigación se dividen en el análisis del comportamiento intrínseco de los dispositivos (fingerprinting), la viabilidad económica de la propuesta y la validación técnica mediante simulaciones de ataque.

Análisis de Comportamiento (Fingerprinting) y Protocolos

El análisis de las capturas de tráfico permitió identificar patrones normales de operación. Se observó que, independientemente de la funcionalidad del dispositivo, los protocolos UDP, TCP y TLS dominan el espectro de comunicación. El tráfico UDP es predominante en la cámara IP debido al streaming de video en tiempo real, mientras que el bombillo y el tomacorriente muestran picos de tráfico TCP/TLS durante la recepción de comandos de la aplicación móvil.

Protocolo Identificado	**Uso Común en Dispositivos IoT**
UDP	Transmisión de video y voz (Cámaras)
TCP	Gestión de estados y comandos de control
TLS (SSL)	Cifrado de la comunicación hacia la nube
ARP / mDNS	Descubrimiento de servicios y resolución local

La interpretación de las direcciones IP reveló que el tráfico se origina principalmente desde servidores centralizados de los fabricantes en regiones geográficas específicas (Estados Unidos, Asia y Europa). Cualquier desviación de estos rangos de IP conocidos es clasificada automáticamente por el sistema como tráfico anómalo.

Viabilidad Económica y Escalabilidad del Sistema

Un hallazgo fundamental de la tesis es que el modelo serverless de AWS permite una implementación de bajo costo para el usuario residencial. El análisis financiero estima que el monitoreo de tres dispositivos básicos tiene un costo operativo aproximado de $0.1074 USD mensuales, lo que representa menos de $1.30 USD anuales.

Proyección de Costos por Escalabilidad en AWS	**Mensajes Facturados**	**Costo Mensual Total (USD)**
3 dispositivos (Base)	43,200	~$0.10
10 dispositivos	43,200	~$0.16
25 dispositivos	86,400	~$0.31

La eficiencia económica se mantiene incluso en hogares con alta densidad de dispositivos, donde el costo mensual sigue siendo altamente viable. Este nivel de escalabilidad es posible gracias a la consolidación de métricas en el gateway local antes del envío a la nube.

Fase de Pruebas y Validación del Sistema

El sistema fue sometido a tres escenarios de ataque reales utilizando herramientas de auditoría en Kali Linux para verificar la efectividad de las reglas de detección configuradas en AWS Lambda:

- **Escaneo ARP Masivo**: Se simuló un descubrimiento de red utilizando nmap -sn -PR. El sistema detectó la generación inusual de paquetes ARP en el gateway local; la función Lambda comparó este volumen con el umbral histórico y envió una alerta inmediata vía Amazon SNS con el diagnóstico de "ARP_SCAN_SUSPECT".
- **Escaneo de Puertos Críticos**: Al ejecutar un escaneo hacia el puerto 22 (SSH), que no se encuentra en la lista de puertos autorizados para los dispositivos IoT analizados, el sistema generó una notificación de alerta indicando un intento de reconocimiento no autorizado.

- **Conexión desde Redes No Reconocidas**: Se intentó acceder a la gestión de los dispositivos desde una dirección IP externa no registrada en la "whitelist". El IDS basado en AWS identificó el origen anómalo y notificó al usuario la presencia de una conexión sospechosa, permitiendo una postura de defensa proactiva.

4. Conclusiones

Esta investigación demuestra que la ciberseguridad en el hogar inteligente no puede depender exclusivamente de los fabricantes de dispositivos ni de los enrutadores residenciales convencionales. La implementación de un sistema de monitoreo basado en una arquitectura híbrida (Edge-Cloud) proporciona una visibilidad granular y una capacidad de detección de amenazas superior a las soluciones tradicionales.

Conclusiones sobre la Infraestructura y Detección

El uso de un gateway local fundamentado en Scapy y Python es una solución técnica eficaz para solventar la incapacidad de procesamiento de los dispositivos domésticos. La transformación de trazas PCAP a objetos estructurados JSON en el borde de la red asegura que solo los metadatos relevantes sean transmitidos, garantizando la eficiencia del ancho de banda y el cumplimiento de principios básicos de privacidad al evitar el envío de contenido sensible a la nube. Asimismo, la arquitectura de AWS IoT permite una gestión centralizada y escalable que reduce drásticamente el tiempo de detección de anomalías y la tasa de falsos positivos en comparación con sistemas de firmas estáticas.

Conclusiones sobre la Postura de Defensa Proactiva

El sistema propuesto desplaza la ciberseguridad residencial de un estado reactivo a uno proactivo. La integración de AWS Lambda como motor de orquestación permite no solo alertar al usuario, sino también sentar las bases para la automatización de la respuesta ante incidentes, como el aislamiento de dispositivos comprometidos en VLANs de cuarentena. Esto es vital para mitigar el riesgo de movimiento lateral, donde un atacante utiliza un dispositivo vulnerable (como un bombillo inteligente) para acceder a activos críticos (como computadoras personales o sistemas de almacenamiento).

Recomendaciones Finales

Se recomienda a las organizaciones y usuarios domésticos en Costa Rica adoptar marcos de referencia internacionales como los controles de seguridad de CIS y el estándar ISO/IEC 27001 para la gestión de activos IoT. A nivel técnico, para la implementación del sistema descrito, es imperativo transicionar hacia el uso de certificados X.509 individuales por dispositivo para evitar que el compromiso de un certificado único comprometa la totalidad de la red.

Se debe tomar en cuenta que, al ser este un prototipo inicial, el uso de una laptop con Windows 10 puede ser una limitante de hardware para soluciones o ambientes de mayor demanda. Esto puede ser abordado utilizando un hardware embebido de bajo costo y consumo, utilizando una distribución Linux endurecida.

Para futuras investigaciones, se sugiere explorar el uso de Inteligencia Artificial Generativa (Amazon Bedrock) para generar reportes en lenguaje natural que faciliten la comprensión de los incidentes para usuarios no técnicos, así como el despliegue de AWS IoT Greengrass para dotar al gateway local de capacidades de detección autónoma incluso ante una desconexión total de Internet. La ciberseguridad residencial debe evolucionar hacia sistemas inteligentes, accesibles y económicamente sostenibles para garantizar la resiliencia de los hogares modernos frente a las crecientes amenazas del entorno digital.

Referencias

Akinpelu, Z. O. (10 de Julio de 2024). *The Looming Threat of Unsecured IoT Devices: A Deep Dive*. Obtenido de ISACA.com: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/the-looming-threat-of-unsecured-iot-devices#:~:text=Weak%20authentication:%20Many%20IoT%20devices%20suffer%20from,security%2C%20leaving%20devices%20susceptible%20to%20unauthorized%20acces

Amazon Web Services. (2026). *Precios de Amazon CloudWatch*. Obtenido de Amazon CloudWatch: https://aws.amazon.com/es/cloudwatch/pricing/

Amazon Web Services. (s.f.). *AWS IoT Device Defender*. Obtenido de https://aws.amazon.com/es/iot-device-defender/

Bitdefender. (2025). *THE 2025 IOT Security Landscape Report.* Obtenido de Bitdefender.com:

https://blogapp.bitdefender.com/hotforsecurity/content/files/2025/10/2025_iot_security_report.pdf

Cloudflare. (s.f.). *¿Qué es TCP/IP?* Obtenido de ¿Qué son IP y TCP?: https://www.cloudflare.com/es-es/learning/ddos/glossary/tcp-ip/

Cloudflare. (s.f.). *¿Qué es TLS (Transport Layer Security)?* Obtenido de https://www.cloudflare.com/es-es/learning/ssl/transport-layer-security-tls/