INVESTIGACIÓN e INNOVACIÓN en INGENERÍAS
ISSN2344-8652

Arquitectura basada en tecnologías emergentes y monitoreo de tráfico de red

Architecture based on emerging technologies and network traffic monitoring

Juan José Caiza Narváez **Katerine Márceles Villalba**

Institución Universitaria Colegio Mayor del Cauca, Colombia

Siler Amador Donado
Universidad del Cauca, Colombia

OPEN ACCESS

Recibido: 22/09/2021
Aceptado: 22/10/2021
Publicado: 13/12/2021

Correspondencia de autores:
juanjosecaiza@unimayor.edu.co

CC BY

Copyrith 2020 by Investigación e Innovación en Ingenierías

Resumen

Objetivo: Describir la estructuración de una arquitectura basada en ciberseguridad para mitigar el tráfico malicioso usando dispositivos IoT. **Metodología:** Para ello se utilizó una metodología basada en 4 fases, de las cuales, se da inicio con la identificación y selección de las tecnologías emergentes que presentan mayor impacto en la ciberseguridad de IoT, seguido de la identificación del algoritmo de inteligencia artificial que presente las características adecuadas a la estructura propuesta, más adelante se determinó la técnica de monitoreo adecuada para realizar la captura y monitorear el tráfico de red en tiempo real que circula por estos dispositivos IoT, para finalmente realizar la determinación de la arquitectura. **Resultados:** Así se obtuvo una arquitectura diseñada bajo tres capas, donde cada capa contiene la selección previa realizada en las respectivas fases. **Conclusiones:** Obteniendo un diseño que permite el monitoreo en tiempo real del tráfico que circula por los dispositivos IoT, considerando el almacenamiento de datos, que posteriormente se procesa bajo el algoritmo de IA(Inteligencia artificial) y determinará la creación de nuevas reglas para notificar posibles amenazas.

Palabras clave: Arquitectura, Ciberseguridad, Inteligencia Artificial, IoT, Tráfico de red.

Abstract

Objective: Describe the structuring of an architecture based on cybersecurity to mitigate malicious network traffic in IoT devices. **Methodology:** For this, a methodology based on 4 phases was used, of which, it begins with the identification and selection of emerging technologies that have the greatest impact on IoT cybersecurity, followed by the identification of the artificial intelligence algorithm that presents The characteristics that best adapt to the proposed structure, later on the appropriate monitoring technique was determined to capture and monitor in real time the traffic that circulates through these IoT devices, to finally make the determination of the architecture. **Results:** In this way, an architecture designed under three layers was obtained, where each layer contains the previous selection made in the respective phases. **Conclusions:** Obtaining a design that allows real-time monitoring of the traffic that circulates through IoT devices, considering data storage, which is subsequently processed under the AI (Artificial Intelligence) algorithm and will determine the creation of new rules to notify possible anomalies.

Keywords: Architecture, Cybersecurity, Artificial Intelligence, IoT, Network Traffic.

Como citar (IEEE): J. Caiza-Narváez., K. Márceles-Villalba., y s. Amador-Donado. "Arquitectura basada en tecnologías emergentes y tecnología de monitoreo de tráfico de red". Investigación e Innovación en Ingenierías, vol. 9, n°3, 18-31, 2021. DOI: https://doi.org/10.17081/invinno.9.3.5340

Introducción

Actualmente el campo de la informática está en constante auge, tomando gran impulso, debido a las diferentes aplicaciones que existen en ámbitos sociales, económicos, de la salud y académicos, esto ha traído consigo que cada vez se haga más uso de herramientas informáticas en los campos ya mencionados, con la implementación y la utilización de la navegación por la red, ya sea para investigación, divulgación, áreas de salud para manejo de datos, entre otras aplicaciones; abriendo así, un sin número de posibilidades para aplicar y desarrollar el área informática, dando solución a diferentes problemáticas y necesidades expuestas, brindando facilidades a la sociedad; sin embargo, también ha generado un aumento en la conectividad y a su vez en el flujo de datos que se presenten, debido a la gran dependencia de la sociedad con la tecnología, lo que ha provocado crecimiento en el riesgo de que los sistemas puedan ser vulnerados. Esto no solo aplica para grandes sistemas, sino que también se expone a los dispositivos IoT, son aquellos que tienen lugar en cada uno de los hogares, por ejemplo: televisores inteligentes, parlantes, juguetes conectados a internet, dispositivos portátiles, electrodomésticos, entre otros, son casos que usualmente no se tienen en cuenta en cuestiones de ciberseguridad y que de hecho estos pueden vulnerarse muy fácilmente dejando expuestos datos e información de importancia.

Es por ello, que se crea la necesidad en generar una protección a este tipo de dispositivos y la seguridad de los datos que puedan tener, ya que brindan la oportunidad a potenciales agresores, dando diversas entradas y siendo vectores para todo tipo de actividades no seguras, en atención a lo cual se identifica la necesidad de implementar medidas de ciberseguridad para dispositivos IoT, trayendo consigo también la acción de la inteligencia artificial que son mecanismos que actualmente se emplean a nivel mundial para diversas actividades en virtud de suplir los vacíos de seguridad que se puedan dar en los sistemas de red, dando pie a que los datos se vulneren, creando a su vez herramientas apropiadas y mecanismos que proporcionen mejores niveles de seguridad, disminuyendo así la brecha de amenazas a los distintos dispositivos.

Esta necesidad surge debido a que en la actualidad los ciber-riesgos ya no son amenazas poco usuales en empresas u organizaciones, de manera que se han constituido como amenazas de alto riesgo en todos los sectores y ámbitos industriales, muchas empresas del sector público y privado buscan mejorar sus sistemas de seguridad invirtiendo grandes cantidades de dinero y buscando académicos que puedan desarrollar alternativas que se ajusten a las necesidades de cada una de estas con el fin de proteger sus datos. No obstante, esto lleva a generar altos costos, que algunas organizaciones no pueden suplir, dejando en riesgo y vulnerables a sus dispositivos, por tal razón, se busca crear una arquitectura IoT, que genere una protección en estos dispositivos, permitiendo analizar el tráfico malicioso de red que pasa por cada uno de ellos y de esa forma dar paso a una verificación para descartar amenazas que se puedan presentar, evitando así que terceros tengan acceso a la información y se presente vulneración de datos.

En el proceso de construcción de la arquitectura adecuada es importante resaltar estudios previos o antecedentes que se tuvieron en cuenta en dicho proceso, en el 2005 en un estudio realizado por H. Tahae [1], a través de una encuesta se analizan las tendencias emergentes sobre la clasificación de tráfico de red malicioso en IoT, de igual forma se estudia la utilización y clasificación del tráfico en sus diferentes aplicaciones; además, se compara el legado de los métodos de clasificación de tráfico y finalmente se presenta una descripción general de los modelos tradicionales, permitiendo así a la investigación tomar como referencia los diferentes métodos de clasificación de tráfico[1].

De igual forma M. Aminu Lawal en el (2020)[2], desarrollan un estudio en donde se propone un marco de mitigación de anomalías híbrido para IoT, el cual utiliza la computación en la red para garantizar una

detección de anomalías más rápida y precisa. En este estudio se emplean metodologías de detección basadas en firmas y anomalías para sus dos módulos. De esta forma el módulo basado en firmas utiliza una base de datos de fuentes de ataque (direcciones IP en lista negra) para garantizar una detección más rápida cuando los ataques se ejecutan desde la dirección IP en la lista negra, mientras que el módulo basado en anomalías utiliza un algoritmo de aumento de gradiente extremo para una clasificación precisa del flujo de tráfico de red en normal o anormal, obteniendo así el resultado de dos metodologías de detección. Con dicho estudio se obtiene información para la evaluación del algoritmo con el fin de analizar de manera más precisa el flujo del tráfico de red[2].

En el estudio realizado por H. Haddad Pajouh en el (2020)[3], se propone una arquitectura segura para la infraestructura de capa de borde de IoT, llamada AI4SAFE-IoT, esta arquitectura se basa en módulos de seguridad impulsados por IA en la capa de borde para proteger la infraestructura de IoT; además, se analiza atribución de amenazas cibernéticas, firewall de aplicaciones web inteligentes, búsqueda de amenazas y la inteligencia sobre ciberamenazas. Son los principales módulos que se proponen en el estudio [3], lo cual resultó relevante puesto que sirve como parte del diseño para la arquitectura del presente artículo.

Finalmente, es importante mencionar el estudio realizado por [4], en donde se diseña y desarrolla una arquitectura de IoT con blockchain e IA para respaldar un análisis de big data efectivo, lo que se resulta en una arquitectura de IoT inteligente habilitada para blockchain que proporciona una forma eficiente de converger con las técnicas y aplicaciones actuales, también presentan una evaluación de desempeño de la arquitectura BlockIoTIntelligence para comparar las investigaciones existentes sobre dispositivos, en el tráfico de red en la capa borde y la inteligencia de algoritmos en la capa nube, de acuerdo con algunos parámetros como precisión, latencia, seguridad y privacidad, complejidad computacional y costo de energía en aplicaciones de IoT[4], resultado relevante para el estudio en la construcción del modelo de arquitectura para la ciberseguridad de IoT.

De este modo, se plantea entonces una arquitectura desarrollada bajo tres capas, Detecction Layer, Cloud Layer, Application Layer, para ello se seleccionó una tecnología de monitoreo, de igual forma, se da uso de un algoritmo de inteligencia artificial y finalmente la tecnología emergente, estos tres parámetros se escogieron teniendo en cuenta su rendimiento, precisión, aportes a la ciberseguridad e innovación, todo enfocado en IoT. Es importante destacar que esta arquitectura es de bajo costo, está basada en tecnologías emergentes de ciberseguridad y trabaja bajo un algoritmo de inteligencia artificial que suele ser poco usual en otros modelos, buscando así mejorar la ciberseguridad en dispositivos IoT.

Metodología

Dentro del marco del desarrollo de la arquitectura IoT, se implementó la metodología investigación-acción, la cual se desarrolló en cuatro fases, que permiten determinar qué tecnologías serán utilizadas para la construcción de dicha arquitectura. Para ello se realizó una investigación exhaustiva a través de la búsqueda de información, con el fin de identificar los estudios más relevantes que posteriormente fueron evaluados y seleccionados bajo unos criterios establecidos, dejando solo los que generen un aporte significativo al objetivo central. Por tanto la arquitectura está encaminada bajo 4 fases como se evidencia a continuación:

Fase 1 Identificación de la tecnología emergente.

Es importante resaltar que las tecnologías emergentes están encaminadas a mejorar el desarrollo de la ciberseguridad de los dispositivos de IoT, por la cual su identificación y correcta elección es clave para la construcción de la arquitectura. Con base en una búsqueda exhaustiva entre las tecnologías más utilizadas en el ámbito de estudio se obtuvo un primer listado, posteriormente se indagó en detalle cada una de estas tecnologías estableciendo así cuales eran las que tenían mayor impacto en el área de ciberseguridad, de este modo se determinó que las mejores son las que se indican en la tabla 1.

Tabla 1. Tecnologías emergentes IoT bajo niveles de ciberseguridad.

TECNOLOGÍAS EMERGENTES
Identity and Access Management as a Service (IDaaS)
Cloud Access Security Brokers (CASBs)
Big Data Security Analytics
Virtualized Firewalls
Threat Intelligence Platforms

Fuente: Propia

IDaaS, tiene como enfoque principal analizar las plataformas de nube de IoT populares a la luz de la solución de varios dominios de servicio, como el desarrollo de aplicaciones, la gestión de dispositivos, la gestión de sistemas, la gestión de heterogeneidad, la gestión de datos, las herramientas para el análisis, la implementación, la supervisión, la visualización y la investigación [5]. Por otra parte, CASBs tiene como objetivo mejorar las características de seguridad y colocando los datos entre la nube pública y sus consumidores, es decir, se usa como una capa intermedia entre la nube y los usuarios finales, la característica de diseño de este estudio es que reduce con éxito el costo de comunicación adicional que generalmente se encuentra alto en sistemas similares[6]. También se tiene a Big Data, la cual vincula los datos de forma segura a través de una puerta de enlace de borde a una llamada nube de sensores, dentro de la puerta de enlace de borde, se aplican mecanismos de detección de intrusiones y los mecanismos de control de acceso que autentican los datos [7]. Del mismo modo, se tiene Virutalized Firewalls la cual proporciona control del acceso no autorizado al dispositivo, integridad sin conexión, autenticación de los datos en la fuente, protección contra varios ataques y confidencialidad mediante el uso de técnicas de cifrado, este control de acceso se puede lograr mediante claves criptográficas[8,9]. Finalmente, se tiene a Threat Intelligence Platforms basada en el análisis de datos, esta tecnología está basada en la detección de intrusiones, que pueden beneficiarse de mecanismos de inteligencia artificial, como el aprendizaje automático con el fin de construir un sistema inteligente basado en datos, aplica algoritmos de aprendizaje automático para analizar y clasificar el contenido del correo electrónico y se defiende activamente contra la ingeniería social [10,11].

Tabla 2. Evaluación de tecnologías emergentes.

TECNOLOGÍAS EMERGENTES	INNOVACIÓN TECNOLÓGICA	CIBERSEGURIDAD	TECNOLOGÍAS IOT	PUNTAJE	VALOR %
Identity and Access Management as a Service (IDaaS)	BUENO	ALTO	BUENO	22,2	73,3%
Cloud Access Security Brokers (CASBs)	ALTO	BUENO	MEDIO	23	76,6%
Big Data Security Analytics	BUENO	ALTO	ALTO	27,5	91,6%
Virtualized Firewalls	ALTO	ALTO	BUENO	26	86,6%
Threat Intelligence Platforms	ALTO	ALTO	ALTO	29	96,65

Fuente: Propia

Ahora bien, para elegir la o las tecnologías apropiadas para el desarrollo de la arquitectura se establecieron varios parámetros como se muestra en la tabla 2, entre los cuales esta la innovación tecnológica, aporte a la ciberseguridad, si están basadas en tecnologías IoT, logrando así determinar las que se ajusten más a los objetivos de la arquitectura. De este modo, se obtuvo Big Data con un puntaje de 91,6 % e Intelligence Platforms con un puntaje de 96,65% son las tecnologías escogidas para el desarrollo de la arquitectura. Big data es la que permite realizar el correcto análisis de los datos e Intelligence Platforms permite monitorear, controlar la información y tráfico que pasa por los dispositivos IoT.

Fase 2: Identificación del algoritmo de IA.

Algunas herramientas tecnológicas no cuentan con mecanismos eficientes para proteger la información, no están desarrolladas bajo parámetros de seguridad y en el caso específico algunas tecnologías IoT no cuentan con mecanismos para proteger la información; por ello, hacer uso de algoritmos inteligentes es un tema importante en esta área, ya que al combinarlos se puede obtener un tráfico controlado más robusto. Para esto se hizo un análisis de un total de 26 algoritmos ver tabla 3.

Tabla 3. Algoritmos de IA.

Algoritmos	Dataset de EVALUACIÓN	Articulo
RBF-SVM	KDD Cup 99	[12]
PSO-SVM	KDD Cup 99	[13]
SVM	NSL-DD, DARPA 1998	[14,15,16]
C-SVM	KDD Cup 99	[17]
IPDS-KNN	NSL-KDD	[18]
KMEANS-KNN	NSL-KDD	[19]
KFN-KNN	NSL-KDD	[20]
KNN	DARPA 1998	[21]
ACO-KNN	KDD Cup 99	[22]
MIX-KNN	KDD Cup 99	[23]
CFS-DT	NSL-KDD	[24]
MULTI-DTS	KDD Cup 99	[25]

C4.5 DT	KDD Cup 99	[26]
CFS-DT	KDD Cup 99	[27]
GA-C45	KDD Cup 99	[28]
DT-KNN	KDD Cup 99	[29]
DT	Netflow	[30,31]
DBN	NetFlow, KDD Cup 99, NSL-KDD.	[32,33,34,35,36]
DBN-PNN	KDD Cup 99	[37]
LR-DBN	KDD Cup 99	[38]
RNN	NSL-KDD	[39,40]
LSTM	KDD Cup 99	[41,42,43]
GRU	Netflow	[44]
CNN	CTU-UNB Dataset, netflow	[45,46,47,48]
ID-CNN	ISCX Dataset	[49]
Ramdon forest	Cicids2017- NDSec1- Cse-CIC-IDS 2018- CIC-DDoS2019	[50]

Fuente: [51]

De los cuales se realizó un primer filtro teniendo en cuenta el nivel de precisión y se determinó un total de 6 algoritmos con los porcentajes más altos. El siguiente paso fue realizar un análisis a los algoritmos bajo los parámetros de precisión, respuesta, recurso, tiempo y puntaje, tomando así el que obtuviese el porcentaje más alto, ver tabla 4.

Tabla 4. Evaluación de Algoritmos de IA.

ALGORITMO	PRECISIÓN	RESPUESTA	RECURSO	TIEMPO	PUNTAJE	VALOR %
PSO-SVM	ALTO	BUENO	MEDIO	INTERMEDIO	22	55%
DBN-PNN	ALTO	BUENO	MEDIO	BAJO	23,6	59%
GA-C45	ALTO	BUENO	MEDIO	MEDIO	25,2	63%
RBF-SVM	ALTO	MEDIO	MEDIO	BAJO	26	65%
DT-KNN	ALTO	BUENO	INTERMEDIO	MEDIO	27,5	68%
RANDOM FOREX	ALTO	ALTO	INTERMEDIO	BAJO	33,6	84%

Fuente: Propia

De esta forma, se tiene PSO-SVM [13], es uno de los métodos más sólidos y precisos de todos los algoritmos de aprendizaje automático, y se evaluó en KDD Cup 99, con un resultado de 99% de precisión. DBN-PNN [32], es un modelo generativo probabilístico que consta de múltiples capas de variables ocultas y estocásticas, este algoritmo se evaluó en el Dataset KDD Cup 99, y se obtuvo un nivel de precisión de 99,14%.

GA-C45 [28], este algoritmo se clasifica como un árbol de decisión, y se define como una estructura de árbol en la que cada nodo interno representa una prueba en una propiedad y cada rama representa una salida de prueba y cada nodo hoja representa una categoría, la prueba de este algoritmo se dió en el Dataset KDD Cup 99 y se obtuvo un nivel de precisión de 99,89%.

RBF-SVM, se utiliza como una función del kernel de SVM para clasificar conjuntos de datos DoS, Probe, U2R y R2L, este algoritmo se evaluó en el Dataset de KDD Cup 99 y arrojó un resultado en el nivel de precisión de 99,9%. DT-KNN, se basa en una función de distancia que mide la diferencia o similitud entre dos instancias, este algoritmo se evaluó con NSL-KDD [29], dando como resultante un 99,9% de precisión, finalmente

RANDOM FOREX, es una combinación de árboles predictores y aleatorios, este algoritmo es evaluado en cuatro bases de datos, CICIDS-2017, ND Sec-1, CSE-CIC IDS-2018, CICDDoS-2019, los resultados obtenidos para los análisis de precisión fueron 99,9%, 100%, 99,9% y 99,9% respectivamente [50].

Considerando los valores obtenidos con base en estos 6 algoritmos que se tomaron como los valores más altos, se seleccionó el algoritmo RANDOM FOREX, inicialmente porque a diferencia del resto de algoritmos en selección, este fue evaluado en 4 bases de datos diferentes, en donde se obtienen resultados cercanos a 100% y en un caso el valor total, brindando mayor confianza en su uso; además, siendo un algoritmo que funciona por clasificación aleatoria, presenta mayor efectividad en su clasificación en el tráfico de red.

Fase 3: Técnica de monitoreo.

Las técnicas de monitoreo son ampliamente utilizadas para monitorear y detectar actividades maliciosas del tráfico de la red, por ello se determina una lista de 5 técnicas de monitoreo en donde se evalúa el análisis de firmas, análisis de anomalías, si permite crear nuevas reglas, consumo de recursos, si maneja software libre y almacenamiento de tráfico, ver tabla 5.

Tabla 5. Tecnologías de monitoreo.

TECNOLOGÍAS DE MONITOREO	ANÁLISIS DE FIRMAS	ANÁLISIS DE ANOMALÍAS	PERMITE CREAR NUEVAS REGLAS	CONSUMO DE RECURSOS	SOFTWARE LIBRE	ALMACENAMIENTO DE TRÁFICO.	PUNTAJE	VALOR %
Suricata	ALTO	ALTO	ALTO	BAJO	SI	SI	58,5	97,5%
Bro (Zeek)	ALTO	ALTO	BAJO	BAJO	SI	SI	55,5	92,2%
Wireshark	ALTO	BUENO	MEDIO	MEDIO	SI	SI	47,5	79%
Tcpdump	ALTO	BUENO	MEDIO	BAJO	SI	SI	49,5	82,5%
Snort	ALTO	ALTO	ALTO	BAJO	SI	SI	56,5	94%
AWS IoT	ALTO	ALTO	BAJO	BAJO	NO	SI	45,5	75%

Fuente: Propia

Determinando así, que el porcentaje más alto lo tienen suricata con 97,5% y snort con 94%, siendo las dos tecnologías de monitoreo con los puntajes más destacados en la presente evaluación; sin embargo, en el proceso de evaluación de rendimiento, suricata generó mejores resultados, considerando que esta tecnología está diseñada bajo análisis de firmas, búsqueda de anomalías, además que para el diseño de la presente arquitectura es importante la generación de nuevas reglas, sumando que tiene tecnología open sourse que permite ser implementado en este escenario, ya que la propuesta está basada en tecnologías de bajo costo.

Fase 4: Determinación de la arquitectura.

Para el desarrollo de la estructura de hardware y software que será utilizada en el marco de esta arquitectura IoT, es importante definir una arquitectura de hardware de bajo costo, estos dispositivos SBC (single board computer) son seleccionados debido a sus características, su disponibilidad y facilidad de compra. Como se puede observar en la tabla 6, se describe cada dispositivo con las siguientes características, el nombre

del dispositivo, frecuencia, núcleos, Memoria RAM, conexión a internet, precio (peso Colombiano) y sistema operativo. Cabe mencionar, que estos precios son una aproximación, dado que en distintos sitios, ofrecen estos dispositivos SBC, a diferentes precios.

Tabla 6. Características de dispositivos hardware.

NO	DISPOSITIVO	FRECUENCIA	NÚCLEOS	RAM	CONEXIÓN INTERNET	PRECIO	SISTEMA OPERATIVO
1	Raspberry Pi Zero	1.0GHz	1	512MB	NO	$130.000	Android, Linux, Windows.
2	Orange pi PC	600MHz	4	1GB	Ethernet	$135.000	Android Ubuntu, Debian, Linux.
3	NanoPi R1	1.2GHz	4	1GB	Wi-Fi, Ethernet.	$142.000	Android, Linux.
4	Raspberry Pi 3	1.8GHz	4	1GB	Wi-Fi, Ethernet.	$160.000	Android, Linux, Windows.
5	Banana Pi M2	1.0GHz	4	1GB	Wi-Fi, Ethernet.	$180.000	Android, Linux.
6	Pine A64 LTS	1.2GHz	4	2GB	Ethernet	$180.000	Android, Linux, Windows.
7	Odroid C2	1.5GHz	4	2GB	Ethernet	$205.000	Android, Linux.
8	Rock Pi 4	1.8GHz	4	2GB	Wi-Fi, Ethernet.	$232.000	Android, Linux, Windows.
9	Orange pi plus 2E	1.8GHz	4	2GB	Wi-Fi, Ethernet.	$250.000	Android, Linux.
10	BeagleBone Black	1.0GHz	1	512MB	Ethernet	$250.000	Android, Linux.
11	Asus Tinker Board S	1.8GHz	4	2GB	Wi-Fi, Ethernet.	$269.000	Linux, Windows.
12	Raspberry pi 4	1.5GHz	4	4GB	Wi-Fi, Ethernet.	$320.000	Android, Linux, Windows.
13	WandBoard Dual	1GHz	2	1GB	Wi-Fi, Ethernet	$367.000	Linux.
14	Latte Panda	1.8GHz	4	2GB	Wi-Fi, Ethernet	$395.000	Linux, Windows.
15	DragonBoard	1.2GHz	4	1GB	WIFI	$400.000	Linux, Windows.
16	nVidia Jetson Nano	1.4GHz	4	4GB	Wi-Fi, Ethernet	$470.000	Android, Ubuntu, Linux.
17	PC- AMD Generic	1.3GHz	1	1G	Ethernet	$450.000	Ubuntu, Linux, Windows

Fuente: Propia

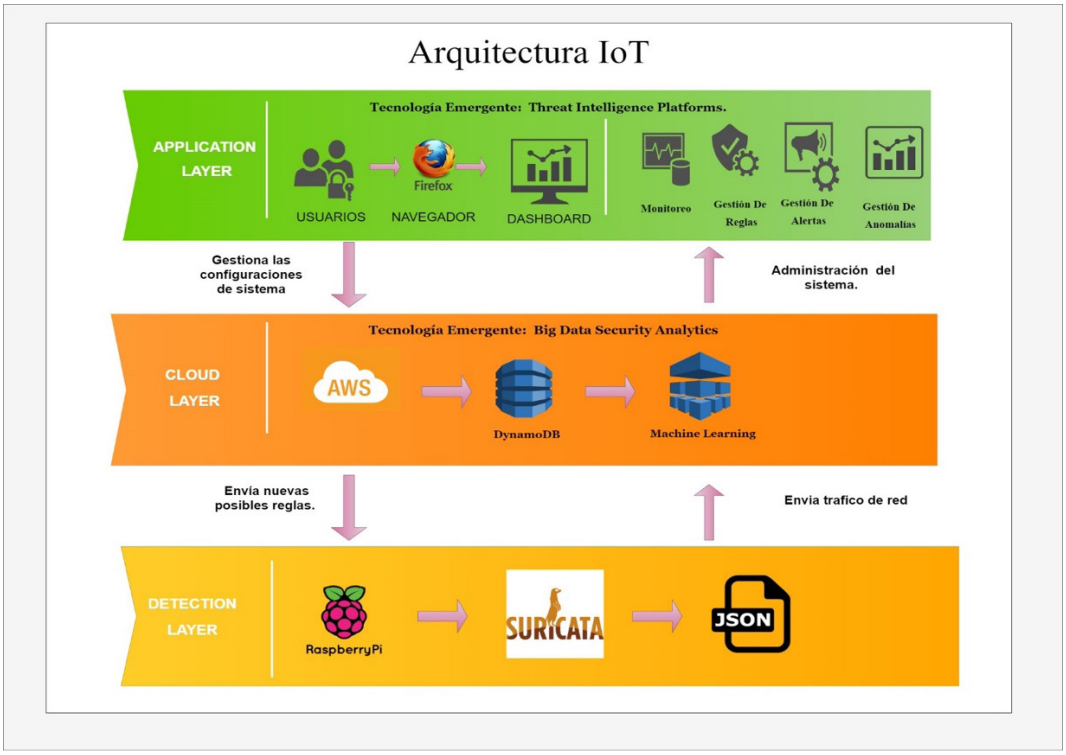
Tomando como base el listado de los dispositivos y cada una de las características descritas en la tabla 6, se establecen unos criterios de evaluación que permitieron determinar cuál es el hardware con las mejores características, por ello se tuvo en cuenta la frecuencia, memoria RAM, núcleos y sistema operativo, los cuales fueron evaluados bajo 6 rangos: muy bajo (0,1 – 1) , bajo (1,1 – 2), intermedio (2,1 – 4), medio (4,1 – 6), bueno 6,1 - 8 y alto (8,1 – 10), de igual forma se tomó en cuenta el precio, el cual se evaluó en 6 rangos: muy bajo de (8,1 – 10), bajo (6,1 – 8), intermedio (4,1 – 6), medio (2,1 – 4) , bueno (1,1 – 2) y alto (0,1 – 1) ; finalmente, se evaluó la conexión a internet, a partir de tres posibilidades: ethernet + wifi (10), ethernet o

wifi (5), ninguno (0). Determinando así, una escala de 0 a 10 para la evaluación final de cada característica, en donde 0 es el valor más bajo y 10 es el valor más alto para cada criterio, una vez realizada la evaluación con base en los criterios y puntuaciones anteriormente mencionados, se determinó que el dispositivo que presenta el puntaje más alto es la Raspberry Pi 3, con un valor de 45,2 puntos. Se resaltan las características de frecuencia con un puntaje de 8,1 siendo de los más altos; de igual forma, los núcleos con 7 puntos, el parámetro de conexión a internet es fundamental, ya que puede establecerla mediante ethernet o wifi, sin dejar de lado que su costo en el mercado es bajo, eligiéndose de este modo el dispositivo en mención.

Resultados

A continuación, se presenta el diseño de la arquitectura elaborada, la cual está estructurada bajo tres capas: Detecction layer, Cloud layer, Application layer. Cada una de ellas contiene las tecnologías evaluadas anteriormente que serán descritas a continuación ver figura 1.

Figura 1. Arquitectura IoT.

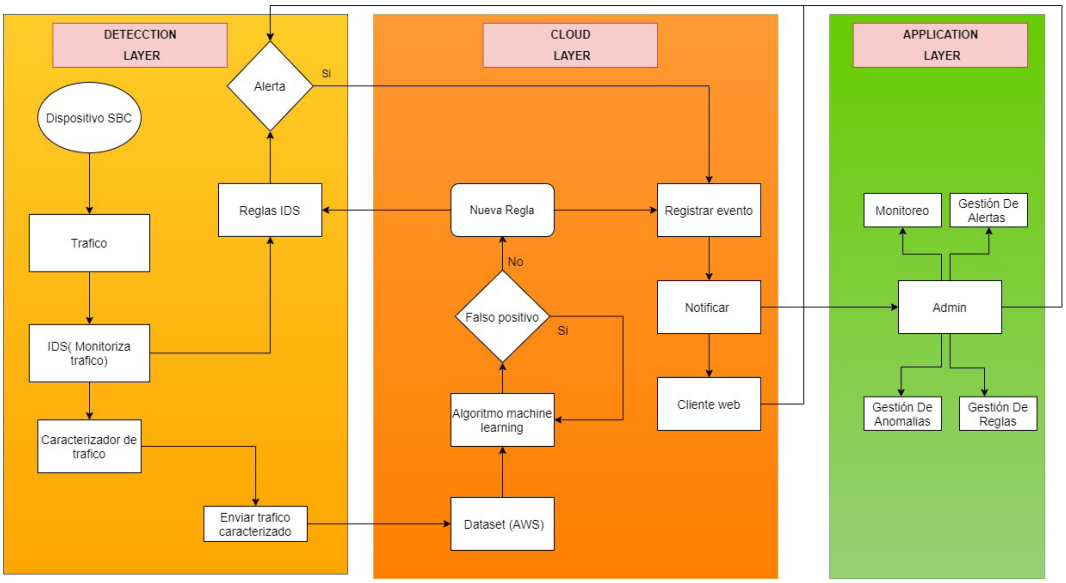


Fuente: Propia

Esta arquitectura está desarrollada bajo tres capas, en el primer nivel, se tiene detection layer, el cual está conformado por tecnologías hardware y software. Para hardware se seleccionó Raspberry Pi 3, por su alta frecuencia , capacidad en núcleos y su conexión a ethernet y wifi. Para software se seleccionó suricata, porque presenta el mejor rendimiento y tiene características propias en su funcionalidad, esta genera archivos JSON, que permiten una lectura más legible del tráfico de red: cabe resaltar, que suricata monitorea en tiempo real el tráfico de red que pasa por cada dispositivo IoT, esta información será enviada a Cloud Layer, esta capa está compuesta de la primera tecnología emergente seleccionada, que es Big data security analytics, esta es la encargada de analizar todos los datos, que serán almacenados bajo un servicio

de AWS, toda esta información es almacenada en una base de datos no relacional denominada DinamoDB, la base de datos se encarga de recibir los documentos convertidos en formato JSON y los almacena. Esta información es más legible para el análisis de tráfico de red, a razón que permite evaluar, analizar y entrenar el algoritmo seleccionado para la generación de nuevas posibles reglas o determinar anomalías en el sistema, este algoritmo RAMDON FOREX está conectado en tiempo real, ya que en la application layer toda la arquitectura tendrá un administrador del sistema, verificando que tanto los dispositivos hardware y software estén en correcto funcionamiento, esto gracias a la tecnología emergente Threat Intelligence Platforms, mediante el panel de control el cual está compuesto por monitoreo, gestión de reglas, alertas y anomalías, a continuación se presenta un diagrama con la descripción más detallada de la arquitectura, ver figura 2.

Figura 2. Modelo funcional de la arquitectura IoT.



Fuente: Propia

En la figura 2, se describe el proceso de acción de la arquitectura IoT, iniciando en detection layer se tiene la arquitectura inicial, en la cual estará conectado un dispositivo SBC (single board computer) con el IDS seleccionado, en este caso es suricata, el cual se le realizan las configuraciones y manejo de reglas. Este software de monitoreo permite capturar el tráfico que transita por los dispositivos IoT, de tal forma que permita enviar una serie de datos hacia capa de cloud layer, donde se encuentra un Dataset que está alojada en AWS, dentro de esta capa estará conectado el algoritmo de machine learning, de tal forma que sea entrenado y configurado para la detección de falsos positivos o falsos negativos y para la creación de posibles reglas que serán enviadas hacia el IDS, este algoritmo además permite analizar las posibles anomalías que detecte en el sistema, para la creación de nuevas reglas; luego la información será registrada como un evento y notificada hacia al cliente o el administrador del sistema, el cual estará en application layer, permitiendo tener un monitoreo en tiempo real del tráfico de estos dispositivos IoT, además de gestionar las anomalías detectadas por el algoritmo y tener un control de las alertas en caso de presentar alguna anomalía, esta información se presentará en gráficos estadísticos que permiten tener un mejor análisis de toda la información.

Conclusiones

Con el alto uso de las redes los datos quedan expuestos, los dispositivos IoT pueden representar una puerta de entrada para intrusos o robo de datos, es por ello la relevancia de la construcción de una arquitectura que mitigue el tráfico e identifique a tiempo cualquier movimiento malicioso, es clave para crear rutas a tiempo que permitan proteger los datos.

En la construcción de una arquitectura es importante tener en cuenta los elementos que la van a componer, en este caso la selección de las tecnologías emergentes, estas deben ser de alto impacto y enfocadas en la temática principal, de igual forma la elección del algoritmo, debe contener las características que cumplan con las necesidades del objetivo propuesto; en este mismo sentido, se debe determinar la técnica de monitoreo adecuada, en virtud que será la encargada de capturar la información y realizar el monitoreo en tiempo real, la selección idónea de estas herramientas es clave para que la arquitectura cumpla el objetivo propuesto.

Agradecimientos

Agradecimientos al grupo de investigación I+D en Informática de la Facultad de Ingeniería de la Institución Universitaria Colegio Mayor del Cauca, por el apoyo y financiamiento brindado para el desarrollo del proyecto, al igual que a la Universidad del Cauca en especial a su grupo de investigación GTI, al semillero de Ciberseguridad y al Ingeniero Christian Urcuqui por las asesorías brindadas.

Referencias Bibliográficas

1. H. Tahaei, F. Afifi, A. Asemi, F. Zaki, and N. B. Anuar, “The rise of traffic classification in IoT networks: A survey,” Journal of Network and Computer Applications, vol. 154. Academic Press, p. 102538, Mar. 15, 2020, https://doi.org/ 10.1016/j.jnca.2020.102538.
2. M. Aminu Lawal, R. Ahmed Shaikh, and S. Raheel Hassan, “An Anomaly Mitigation Framework for IoT Using Fog Computing,” mdpi.com, 2020, https://doi.org/ 10.3390/electronics9101565.
3. H. HaddadPajouh, R. Khayami, A. Dehghantanha, K. K. R. Choo, and R. M. Parizi, “AI4SAFE-IoT: an AI-powered secure architecture for edge layer of Internet of things,” Neural Comput. Appl., vol. 32, no. 20, pp. 16119–16133, Oct. 2020, https://doi.org/ 10.1007/s00521-020-04772-3.
4. S. K. Singh, S. Rathore, and J. H. Park, “BlockIoTIntelligence: A Blockchain-enabled Intelligent IoT Architecture with Artificial Intelligence,” Futur. Gener. Comput. Syst., vol. 110, pp. 721–743, Sep. 2020, https://doi.org/ 10.1016/j.future.2019.09.002.
5. A. Gómez-Cárdenas, X. Masip-Bruin, E. Marín-Tordera, and S. Kahvazadeh, “A novel and scalable naming strategy for IoT scenarios,” in Advances in Intelligent Systems and Computing, Nov. 2019, vol. 880, pp. 122–133, https://doi.org/ 10.1007/978-3-030-02686-8_10.
6. M. Ahmad, M. B. Amin, S. Hussain, B. H. Kang, T. Cheong, and S. Lee, “Health Fog: a novel framework for health and wellness applications,” J. Supercomput., vol. 72, no. 10, pp. 3677–3695, Oct. 2016, https://doi.org/ 10.1007/s11227-016-1634-x.
7. P. Empl and G. Pernul, “A flexible Security Analytics Service for the Industrial IoT; A flexible Security Analytics Service for the Industrial IoT,” vol. 10, 2021, https://doi.org/ 10.1145/3445969.3450427.

8. A. R. Mathew and A. Al Hajj, “Secure Communications on IoT and Big Data,” Indian J. Sci. Technol., vol. 10, no. 11, 2017, https://doi.org/ 10.17485/ijst/2017/v10i11/107974.

9. I. Farris, T. Taleb, Y. Khettab, and J. Song, “A survey on emerging SDN and NFV security mechanisms for IoT systems,” IEEE Commun. Surv. Tutorials, vol. 21, no. 1, pp. 812–837, Jan. 2019, https://doi.org/ 10.1109/COMST.2018.2862350.

10. A. de Melo e Silva, J. J. C. Gondim, R. de Oliveira Albuquerque, and L. J. G. Villalba, “A methodology to evaluate standards and platforms within cyber threat intelligence,” Futur. Internet, vol. 12, no. 6, p. 108, Jun. 2020, https://doi.org/ 10.3390/fi12060108.

11. S. Bauer, D. Fischer, C. Sauerwein, S. Latzel, D. Stelzer, and R. Breu, “Towards an Evaluation Framework for Threat Intelligence Sharing Platforms,” Hawaii Int. Conf. Syst. Sci. 2020, Jan. 2020, Accessed: Mar. 12, 2021. [Online]. Available: https://aisel.aisnet.org/hicss-53/dg/cybersecurity_and_government/3.

12. M. Kotpalliwar, R. W.-2015 F. I. Conference, and undefined 2015, “Classification of Attacks Using Support Vector Machine (SVM) on KDDCUP’99 IDS Database,” ieeexplore.ieee.org, 2015, Accessed: Mar. 11, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7280066/.

13. H. Saxena, V. R.-I. J. of C. Applications, and undefined 2014, “Intrusion detection in KDD99 dataset using SVM-PSO and feature reduction with information gain,” Citeseer, 2014, Accessed: Mar. 11, 2021. [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.680.5101&rep=rep1&type=pdf.

14. M. Shakil Pervez and D. M. Farid, “Feature selection and intrusion classification in NSL-KDD cup 99 dataset employing SVMs,” ieeexplore.ieee.org, 2015, https://doi.org/ 10.1109/SKIMA.2014.7083539.

15. M. Yan and Z. Liu, “A new method of transductive SVM-based network intrusion detection,” in IFIP Advances in Information and Communication Technology, 2011, vol. 344 AICT, no. PART 1, pp. 87–95, https://doi.org/ 10.1007/978-3-642-18333-1_12.

16. R. Kokila, ... S. S.-2014 S. I., and undefined 2014, “DDoS detection and analysis in SDN-based environment using support vector machine classifier,” ieeexplore.ieee.org, 2015, Accessed: Mar. 11, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7229711/.

17. ... A. C.-... on C. and and undefined 2014, “Confederation of fcm clustering, ann and svm techniques to implement hybrid nids using corrected kdd cup 99 dataset,” ieeexplore.ieee.org, 2014, Accessed: Mar. 11, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6949927/.

18. B. Rao and K. S. Science, “Fast kNN classifiers for network intrusion detection system,” sciresol.s3.us-east-2.amazonaws ..., 2017, https://doi.org/ 10.17485/ijst/2017/v10i14/93690.

19. S. A. A. AM Sharifi, “Intrusion detection based on joint of K-means and KNN - Google Académico,” 2015. https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=Intrusion+detection+based+on+joint+of+K-means+and+KNN&btnG= (accessed Mar. 11, 2021).

20. H. Shapoorifard and P. Shamsinejad, “Intrusion Detection using a Novel Hybrid Method Incorporating an Improved KNN,” 2017. Accessed: Mar. 11, 2021. [Online]. Available: https://fardapaper.ir/mohavaha/uploads/2018/08/Fardapaper-Intrusion-Detection-using-a-Novel-Hybrid-Method-Incorporating-an-Improved-KNN.pdf.

21. W. Meng, W. Li, and L.-F. Kwok, “Design of intelligent KNN-based alarm filter using knowledge-based alert verification in intrusion detection,” Networks, vol. 8, no. 18, pp. 3883–3895, Dec. 2015, https://doi.org/ 10.1002/sec.1307.

22. V. S. A. T. S Vishwakarma, “An intrusion detection system using KNN-ACO algorithm - Google Académico,” 2017. https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=An+intrusion+detection+system+using+KNN-ACO+algorithm&btnG= (accessed Mar. 11, 2021).

23. E. G. Dada, “A Hybridized SVM-kNN-pdAPSO Approach to Intrusion Detection System,” 2017. Accessed: Mar. 11, 2021. [Online]. Available: https://fardapaper.ir/mohavaha/uploads/2018/07/Fardapaper-A-Hybridized-SVM-kNN-pdAPSO-Approach-to-Intrusion-Detection-System.pdf.
24. B. Ingre, A. Yadav, and A. K. Soni, “Decision tree based intrusion detection system for NSL-KDD dataset,” in Smart Innovation, Systems and Technologies, 2018, vol. 84, pp. 207–218, https://doi.org/10.1007/978-3-319-63645-0_23.
25. A. J. Malik and F. A. Khan, “A hybrid technique using binary particle swarm optimization and decision tree pruning for network intrusion detection,” Cluster Comput., vol. 21, no. 1, pp. 667–680, Jun. 2018, https://doi.org/ 10.1007/s10586-017-0971-8.
26. N. Relan, D. P.-2015 I. C. on, and undefined 2015, “Implementation of network intrusion detection system using variant of decision tree algorithm,” ieeexplore.ieee.org, 2015, Accessed: Mar. 11, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7029925/.
27. A. Akintola et al., “Gain Ratio and Decision Tree Classifier for Intrusion Detection,” Artic. Int. J. Comput. Appl., vol. 126, no. 1, pp. 975–8887, 2015, https://doi.org/ 10.5120/ijca2015905983.
28. C. Azad and V. Kumar Jha, “Computer Network and Information Security,” Comput. Netw. Inf. Secur., vol. 8, pp. 56–71, 2015, https://doi.org/ 10.5815/ijcnis.2015.08.07.
29. A. Balogun, A. O. & Balogun, and R. G. Jimoh, “Anomaly Intrusion Detection Using an Hybrid Of Decision Tree And K-Nearest Neighbor Recent Advances in data mining: Twitter mining View project Anomaly Intrusion Detection Using an Hybrid Of Decision Tree And K-Nearest Neighbor,” 2015. Accessed: Mar. 11, 2021. [Online]. Available: https://www.researchgate.net/publication/282326950.
30. A. A.-J. of C. and Communications and undefined 2015, “A decision tree classifier for intrusion detection priority tagging,” scirp.org, 2015, Accessed: Mar. 11, 2021. [Online]. Available: https://www.scirp.org/html/6-1730195_55717.htm.
31. D. Moon, H. Im, I. Kim, J. P.-T. J. of supercomputing, and undefined 2017, “DTB-IDS: an intrusion detection system based on decision tree using behavior analysis for preventing APT attacks,” Springer, 2017, Accessed: Mar. 11, 2021. [Online]. Available: https://link.springer.com/content/pdf/10.1007/s11227-015-1604-8.pdf.
32. Y. Ding, S. Chen, J. X.-2016 I. J. C. on, and undefined 2016, “Application of deep belief networks for opcode based malware detection,” ieeexplore.ieee.org, 2016, Accessed: Mar. 11, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7727705/.
33. M. Nadeem, O. Marshall, S. Singh, X. Fang, and X. Yuan, “Semi-Supervised Deep Neural Network for Network Intrusion Detection,” 2016. Accessed: Mar. 11, 2021. [Online]. Available: https://digitalcommons.kennesaw.edu/ccerphttps://digitalcommons.kennesaw.edu/ccerp/2016/Practice/2.
34. F. Qu, J. Zhang, Z. Shao, and S. Qi, “An intrusion detection model based on deep belief network,” in ACM International Conference Proceeding Series, Dec. 2017, pp. 97–101, https://doi.org/10.1145/3171592.3171598.
35. M. Alom, ... V. B.-2015 N. A., and undefined 2015, “Intrusion detection using deep belief networks,” ieeexplore.ieee.org, 2015, Accessed: Mar. 11, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7443094/.
36. Q. Tan, W. Huang, and Q. Li, “An intrusion detection method based on DBN in ad hoc networks,” Aug. 2016, pp. 477–485, https://doi.org/ 10.1142/9789813140011_0056.
37. G. Zhao, C. Zhang, L. Z.-2017 I. International, and undefined 2017, “Intrusion detection using deep belief network and probabilistic neural network,” ieeexplore.ieee.org, 2017, Accessed: Mar. 11, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8005871/.

38. K. Alrawashdeh, C. P.-2016 15th I. international, and undefined 2016, "Toward an online anomaly intrusion detection system based on deep learning," ieeexplore.ieee.org, 2016, Accessed: Mar. 11, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7838144/.

39. C. Yin, Y. Zhu, J. Fei, X. H.-I. Access, and undefined 2017, "A deep learning approach for intrusion detection using recurrent neural networks," ieeexplore.ieee.org, 2017, Accessed: Mar. 11, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8066291/.

40. N. R. RB Krishnan, "'An intellectual intrusion detection system model... -Google Académico," 2016.https://scholar.google.es/scholar?hl=es&as_An+intellectual+intrusion+detection+system+model+for+attacks+classification+using+RNN&btnG= (accessed Mar. 11, 2021).

41. S. Althubiti, W. Nick, J. Mason, ... X. Y.-S., and undefined 2018, "Applying long short-term memory recurrent neural network for intrusion detection," ieeexplore.ieee.org, Accessed: Mar. 11, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8478898/.

42. J. Kim, J. Kim, H. Thu, H. K.-2016 I. Conference, and undefined 2016, "Long short term memory recurrent neural network classifier for intrusion detection," ieeexplore.ieee.org, 2016, Accessed: Mar. 11, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7456805/.

43. G. Kim, H. Yi, J. Lee, Y. Paek, and S. Yoon, "LSTM-Based System-Call Language Modeling and Robust Ensemble Method for Designing Host-Based Intrusion Detection Systems," Nov. 2016, Accessed: Mar. 11, 2021. [Online]. Available: http://arxiv.org/abs/1611.01726.

44. A. M. Fred Agarap, "A Neural Network Architecture Combining Gated Recurrent Unit (GRU) and Support Vector Machine (SVM) for Intrusion Detection in Network Traffic Data ACM Reference Format: Abien Fred M. Agarap. 2018. A Neural Network Architecture Combin-ing Gated Recurrent Unit (GRU) and Support Vector Machine (SVM) for Intrusion Detection in Network Traffic Data," dl.acm.org, pp. 26–30, Feb. 2018, https://doi.org/ 10.1145/3195106.3195117.

45. Y. Yu, J. Long, Z. C.-S. and C. Networks, and undefined 2017, "Network intrusion detection through stacking dilated convolutional autoencoders," hindawi.com, 2017, Accessed: Mar. 11, 2021. [Online]. Available: https://www.hindawi.com/journals/scn/2017/4184196/abs/.

46. B. Kolosnjaji, A. Zarras, G. Webster, and C. Eckert, "Deep learning for classification of malware system call sequences," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2016, vol. 9992 LNAI, pp. 137–149, https://doi.org/ 10.1007/978-3-319-50127-7_11.

47. J. Saxe and K. Berlin, "EXpose: A character-level convolutional neural network with embeddings for detecting malicious URLs, file paths and registry keys," arXiv. arXiv, Feb. 27, 2017.

48. X. Zeng, W. Wang, M. Zhu, X. Ye, and Y. Sheng, "Malware traffic classification using convolutional neural network for representation learning," ieeexplore.ieee.org, 2017, https://doi.org/ 10.1109/ICOIN.2017.7899588.

49. X. Zeng, W. Wang, M. Zhu, J. Wang, and Z. Yang, "End-to-end encrypted traffic classification with one-dimensional convolution neural networks," ieeexplore.ieee.org, 2017, https://doi.org/ 10.1109/ISI.2017.8004872.

50. B. Charyyev and M. H. Gunes, "IoT Event Classification Based on Network Traffic," Aug. 2020, pp. 854–859, https://doi.org/ 10.1109/infocomwkshps50562.2020.9162885.

51. Y. Wu, D. Wei, and J. Feng, "Network Attacks Detection Methods Based on Deep Learning Techniques: A Survey," Secur. Commun. Networks, vol. 2020, pp. 1–17, Aug. 2020, https://doi.org/ 10.1155/2020/8872923.