Como citar este artículo: J. J. C. Narváez, K. Márceles Villalba and S. A. Donado, "Systematic Review for the Construction of an Architecture With Emerging IoT Technologies, Artificial Intelligence Techniques, Monitoring and Storage of Malicious Traffic," in IEEE Revista Iberoamericana de Tecnologias del Aprendizaje, vol. 17, no. 4, pp. 386-392, Nov. 2022, doi: 10.1109/RITA.2022.3217183.

Revisión sistemática para la construcción de una arquitectura con tecnologías emergentes IoT, técnicas de inteligencia artificial, monitoreo y almacenamiento de tráfico malicioso

Juan José Caiza Narváez, Katerine Márceles Villalba, Siler Amador Donado

Abstract- This article presents a systematic review to determine the guidelines that allow the construction of an architecture based on emerging IoT technologies, artificial intelligence techniques, monitoring and storage of malicious traffic, in order to safeguard information, given that there are security flaws in IoT devices, which are intercepted by malicious systems that perform unwanted actions without the consent of the user, causing damage and theft of data, that is why three phases were established to carry out: in the first phase an exhaustive search of information was carried out in specialized databases, where they are selected and classified for the development of the guidelines, in the second phase the information collected was identified and analyzed to define an appropriate algorithm for the study, emerging technologies and key components of the cybersecurity system and finally in the third phase defined the necessary and pertinent guidelines for the struction of an architecture based on emerging technologies.

***Index Terms— cybersecurity, artificial intelligence, network traffic, emerging technology, architecture*.**

I. Introducción

En la actualidad el desarrollo informático ha tomado gran impulso pues va de la mano con las necesidades y demandas que la sociedad manifieste, esto lleva a que se generen actualizaciones y avances continuamente respecto a los diferentes ámbitos en donde tiene cabida, tanto en: lo social, económico, académico e incluso en el campo cultural. Una de las aplicaciones que este continuo desarrollo trajo consigo, es la implementación de la navegación por la red, la cual inicialmente se daba uso y desarrollaba más específicamente en investigaciones relacionadas a entidades gubernamentales [1].

El desarrollo de la navegación en internet trae consigo la creación de herramientas que facilitan las necesidades para la sociedad, pero esto también implica que la conectividad aumente, debido a la dependencia de la sociedad a la tecnología; de igual forma, incrementa el riesgo de que los sistemas sean vulnerados colocando en riesgo información personal y confidencial [2].

J. Caiza Narvaez, Facultad de Ingeniería, Institución Universitaria Colegio Mayor del Cauca, Carrera 7 N° 2-34 Edificio Bicentenario, 190003, Popayán-Cauca, Colombia (juanjosecaizanarvaez@unimayor.edu.co).

K. Márceles Villalba, Facultad de Ingeniería, Institución Universitaria Colegio Mayor del Cauca, Carrera 7 N° 2-34 Edificio Bicentenario, 190003, Popayán- Cauca, Colombia (kmarceles@unimayor.edu.co).

S. Amador Donado, Facultad de Ingeniería Electrónica y Telecomunicaciones, Universidad del Cauca, Carrera 2 #4N-140, 190003, Popayán- Cauca, Colombia (samador@unicauca.edu.co).

DOI (Digital Object Identifier) Pendiente

El desarrollo de la navegación en internet trae consigo la creación de herramientas que facilitan las necesidades para la sociedad, pero esto también implica que la conectividad aumente, debido a la dependencia de la sociedad a la tecnología; de igual forma, incrementa el riesgo de que los sistemas sean vulnerados colocando en riesgo información personal y confidencial [2]. Ahora bien, la mayor difusión de los sistemas de información se da con base al internet de las cosas (IoT), si bien hubo alrededor de 9 mil millones de dispositivos IoT conectados en 2017 y 10 mil millones en 2018, Business Insider proyecta que habrá más de 64 mil millones de dispositivos IoT conectados para el año 2025[3]. Considerando el lugar que tienen cada uno de estos dispositivos (por ejemplo: televisores inteligentes, parlantes inteligentes, juguetes conectados, dispositivos portátiles, electrodomésticos inteligentes, entre otros) en los hogares, oficinas, empresas, etc. Estos dispositivos inteligentes no están construidos teniendo en cuenta un nivel de ciberseguridad, de modo que pueden explotarse muy fácilmente mediante diferentes técnicas que permiten vulnerar el nivel de seguridad.

Es importante hacer mención que en la actualidad la ciberseguridad e inteligencia artificial se emplean a nivel mundial para cualquier actividad, en virtud de que en la sociedad se tiene como una utilidad extrema, por lo que a términos de eficiencia se refiere, se han creado nuevos métodos o herramientas que proporcionan niveles de seguridad muy altos; no obstante, también se puede dejar entrever algunas amenazas a la discreción y a la seguridad, es por ello y con base al sin fin de riesgos que pueden correr los usuarios haciendo uso de estos sistemas, se busca desarrollar una arquitectura basada en algoritmos inteligentes, esto a partir de una búsqueda avanzada y exhaustiva de literatura, con el fin de identificar las tecnologías emergentes que permitan mitigar y monitorear en tiempo real el tráfico malicioso que se puede presentar en los dispositivos IoT.

II. CONCEPTUALIZACIONES

En el marco de los avances informáticos se encuentra el desarrollo de arquitecturas encaminadas a la ciberseguridad; por consiguiente es pertinente mencionar una serie de conceptos claves que contextualicen los lineamientos para la construcción de la arquitectura, como primera medida definir la inteligencia artificial (IA), esta es una rama de las ciencias computacionales enfocada al estudio del aprendizaje en modelos de cómputo con base en dos de sus características primordiales: el razonamiento y la conducta [4]. No obstante, la IA va directamente relacionado con la evolución que han tenido las tecnologías emergentes, las cuales son: herramientas, innovaciones y avances en diferentes sectores.

En este mismo orden de ideas, se propone que las tecnologías emergentes son organismos en constante cambio que examinan ciclos de sobre expectación al tiempo que son disruptivas, todavía no han sido completamente comprendidas ni tampoco suficientemente investigadas [5], por ello es importante resaltar el concepto del internet de las cosas (IoT), el cual es una arquitectura que se caracteriza por ser emergente basada en la Internet lo que facilita la reciprocidad de bienes y servicios entre redes de la cadena de suministro y que tiene un impacto importante en la seguridad y privacidad de los actores involucrados [6]. Todos estos conceptos van entrelazados y encaminados para el estudio del tráfico de red y los procesos que se lleven a cabo para escuchar y analizar el tráfico, para tener una comprensión dentro de las redes de comunicación e identificar comportamientos anómalos, quiebres en la seguridad, analizar el funcionamiento de las aplicaciones y construir planes de acción [7].

III. TRABAJOS RELACIONADOS

En este espacio se presentan los trabajos relacionados con la investigación, los cuales se encuentran enmarcados en la temática de tecnologías emergentes entre ellas: inteligencia artificial, frameworks de ciberseguridad, análisis de tráfico e Internet de las cosas en la industria (IIoT).

En el estudio realizado por H. Tahae en [8], quien por medio de una encuesta permite analizar las tendencias emergentes sobre la clasificación de tráfico de red en IoT; así mismo, 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 [8].

De igual forma M. Aminu Lawal en [9], 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 respectivamente, 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 con el fin de precisar en la identificación del flujo de tráfico de red en normal o anormal, obteniendo así el resultado de dos metodologías de detección. Con este estudio se obtiene información para la evaluación del algoritmo con el fin de analizar de manera más precisa el flujo del tráfico de red [9].

En el estudio realizado por H. Haddad Pajouh en [10], plantea 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 la atribución de amenazas cibernéticas, firewall de aplicaciones web inteligente, búsqueda de amenazas y la inteligencia sobre ciberamenazas. Son los principales módulos que se proponen en el estudio [10], lo cual resultó relevante puesto que sirve como parte del diseño para la arquitectura del presente artículo.

Finalmente, el estudio realizado por S. K. Singh en [11], 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 con inteligencia artificial que proporciona una forma eficiente de converger blockchain e IA para IoT con las técnicas y aplicaciones de vanguardia actuales. Además muestra una evaluación de desempeño de la arquitectura BlockIoTIntelligence para comparar las investigaciones existentes sobre dispositivos en el tráfico de red a borde y la inteligencia de algoritmos en la nube, a partir de algunos parámetros como: precisión, latencia, seguridad y privacidad, complejidad computacional y costo de energía en aplicaciones de IoT [11], siendo referentes para el estudio en la construcción del modelo de arquitectura para la ciberseguridad de IoT.

IV. DESARROLLO METODOLÓGICO

Este artículo analiza y evalúa diferentes estudios con el fin de identificar tecnologías emergentes y así desarrollar una arquitectura ideal para mitigar el tráfico de red malicioso. Esto se llevó a cabo a través de una revisión bibliográfica sistemática, donde se presentan 3 fases: una es la búsqueda avanzada de información, la segunda es la identificación de la información, para luego en la tercera fase realizar su respectivo análisis con el fin de establecer los lineamientos de construcción de una arquitectura para tecnologías emergentes IoT, técnicas de inteligencia artificial y tecnologías de monitoreo y almacenamiento de tráfico malicioso más utilizadas.

Fase 1: Búsqueda avanzada de información.

Se realizó una exhaustiva revisión bibliográfica de la literatura sobre un conjunto de bases de datos bibliográficas, con el fin de obtener artículos en español, inglés y portugués.

Para realizar esta investigación se seleccionaron bases de datos que tuvieran las siguientes características: motor de bases de datos bibliográficas basado en la web y búsquedas por palabras claves con temas relacionados en Ciberseguridad, Internet de las cosas (IoT), Arquitecturas IoT, Trafico de red, Inteligencia artificial.

Ahora bien, con respecto al proceso de selección este se realizó basado en la gestión y desarrollo de proyectos de investigación distribuida en ingeniería de software mediante investigación-acción, donde se establecieron seis fases presentadas en el diagrama de la figura 1 [12], siendo el primer parámetro la búsqueda en las bases de datos bibliográficas a partir de las cadenas de búsqueda, ("Cybersecurity" + "IoT Devices" + "Artificial Intelligence" + "Network Traffic", "Dataset"+ "IoT Architecture" + "Emerging Technologies") y palabras claves como operadores boléanos AND, OR y sus respectivos sinónimos, se combinaron cada una de las palabras claves y se seleccionaron una serie de estudios de los cuales se evaluaron los artículos primarios sobre criterios establecidos, para posteriormente eliminar los estudios no

relacionados.

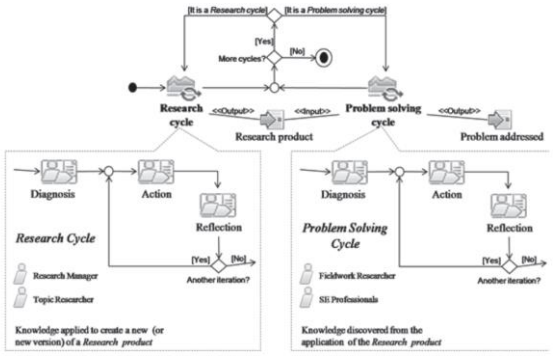

Fig.1. Diagrama de actividades del proceso de investigación para la aplicación de la Investigación-Acción [12]

Luego de realizar la búsqueda por las bases de datos bibliográficas, propuestas en la Tabla I, se evidencia que el número de estudios encontrados es de 109 documentos en total, de los cuales 98 fueron estudios no repetidos. Sin embargo, luego de evaluar estos documentos con base a criterios establecidos se puede evidenciar que 68 estudios son relevantes para el presente caso de estudio; sin embargo, luego de una revisión minuciosa 55 documentos son primarios.

Tabla I. Lista de bases de datos y estudios encontrados.

Bases de datos	**Encontrados**	**No repetidos**	**Relevantes**	**Primarios**
Springer	13	13	10	8
Science@Direct	17	16	13	13
IEEE Xplore	21	19	12	12
ACM Digital Library	8	7	6	1
MDPI	9	9	4	4
Hindawi	6	6	4	2
ResearchGate	10	9	5	2
Otros	25	19	14	17
Total	109	98	68	55

Fuente: Propia

Para realizar la definición de algunos aspectos en el proceso de la revisión de la literatura se tuvo en cuenta las palabras claves, los conceptos y el contexto de la investigación para una comprensión más detallada de cada estudio seleccionado, donde cada actividad proporciona la identificación de los siguientes aspectos: escenarios de destino, dispositivos IoT, inteligencia artificial, tráfico de red, arquitectura; además, de identificar los tipos de investigación: estudio empírico, estudio experimental, pruebas de concepto, experiencia industrial, teórica y caso de estudio; tipo de contribución: metodología, técnica, herramienta, enfoque, modelo, método, estrategia y revisión de la literatura. Esta clasificación se puede ver en la figura 2.

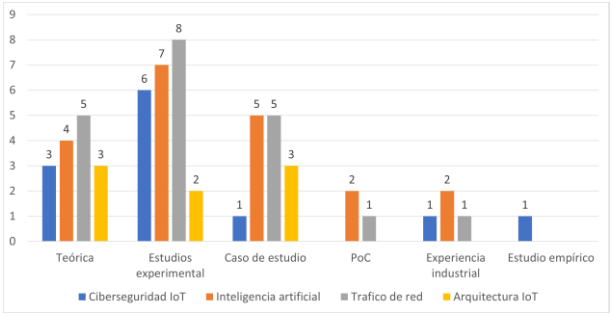

Fig.2. Gráfico de barras de los estudios registrados y palabras claves. Fuente: Propia

Fase 2: Identificación de la información recolectada.

Es importante establecer parámetros de seguridad, ya que existen algunas tecnologías IoT que no cuentan con mecanismos para proteger la información; así que, al hacer uso de algoritmos inteligentes puede generar una diferencia significativa en la seguridad, debido a que al combinarlos se puede obtener un tráfico controlado más robusto [13], siendo así éste el primer parámetro obtenido en la fase 2, ahora bien, esto va ligado a la identificación de tecnologías emergentes IoT en ciberseguridad, ya que puede aportar a la estructura de los lineamientos, siendo esta un segundo parámetro. De igual manera, se buscó identificar las tecnologías que han sido más utilizadas para el monitoreo y almacenamiento de tráfico malicioso, siendo este un tercer parámetro.

Para la identificación del primer parámetro se tiene en la tabla III, un listado con el compendio resultante de la búsqueda avanzada de estudios de algoritmos, que fueron recolectados y evaluados de distintos autores en términos de ciberseguridad, en ella se describe el nombre, así como el Dataset en el cual fueron evaluados y el nivel de precisión que presentaron en cada caso.

Como primera medida se seleccionó un listado de 26 algoritmos, los cuales se componen de una comparación y evaluación mediante bases de datos de tráfico de red y los registros de auditoría recopilados en una red de simulación, entre los cuales están: KDD Cup 99, NSL-DD, DARPA 1998, NSL KDD, Netflow, CTU-UNB, ISCX, CICIDS-2017, ND Sec-1, CSE-CIC IDS-2018, CICDDoS-2019, el compendio de las evaluaciones recolectadas en los diferentes Dataset, se llevaron a cabo con el objetivo de determinar la precisión de cada algoritmo, resultando valores entre 81% hasta 99,9% y 100% para algunos casos. Posterior a la recolección y ejecución del listado, analizando los valores más altos y comparando en los diferentes Dataset se eligieron los 5 valores más altos para una nueva filtración, llegando así al algoritmo del valor mejor valorado, teniendo en cuenta el nivel de precisión y el Dataset donde fue evaluado.

Luego, se realizó la identificación de tecnologías emergentes basadas en ciberseguridad de IoT, esta identificación se hizo de acuerdo con una búsqueda exhaustiva de bibliografía y una posterior filtración de información relacionada a la temática, para ello se utilizaron algunos parámetros a tener en cuenta, entre ellos: las palabras clave, dando peso a las tecnologías más actualizadas, esta elección se da con base a unas características específicas que son mencionadas en la sección de análisis. Es importante, hacer énfasis que las

tecnologías emergentes escogidas aportan en medida al presente estudio. Estas se recopilan junto con los estudios de los cuales se identificaron en la tabla II.

Tabla II. Tecnologías emergentes IoT bajo niveles de ciberseguridad.

Tecnologías Emergentes	Estudio
Identity and Access Management as a Service (IDaaS)	[14]-[15] [16]-[17]
Cloud Access Security Brokers (CASBs)	[18]
Big Data Security Analytics	[19][20]
Virtualized Firewalls	[57] [58]
Threat Intelligence Platforms	[23]-[24]

Fuente propia

Tabla III. Identificación y evaluación de algoritmos [25].

ALGORITMOS	DATASET DE EVALUACIÓN	NIVEL DE PRECISIÓN	ESTUDIO
RBF-SVM	KDD Cup 99	99.9 %	[26]
PSO-SVM	KDD Cup 99	99.0 %	[27]
SVM	NSL-DD, DARPA 1998	80.1%	[28]- [29]-[30]
C-SVM	KDD Cup 99	98.9 %	[31]
IPDS-KNN	NSL-KDD	99.6 %	[32]
KMEANS-KNN	NSL-KDD	90%	[33]
KFN-KNN	NSL-KDD	99%	[34]
KNN	DARPA 1998	85.2%	[35]
ACO-KNN	KDD Cup 99	94.7 %	[36]
MIX-KNN	KDD Cup 99	98.55 %	[37]
CFS-DT	NSL-KDD	90.3 %	[38]
MULTI-DTS	KDD Cup 99	91.94 %	[39]
C4.5 DT	KDD Cup 99	98.45%	[40]
CFS-DT	KDD Cup 99	94.5 %	[41]
GA-C45	KDD Cup 99	99.89 %	[42]
DT-KNN	KDD Cup 99	100 %	[43]
DT	Netflow	84,7%	[44]-[45]
DBN	Netflow, KDD Cup 99, NSL-KDD.	93.49%	[46]-[47]-[48] [49]-[50]
DBN-PNN	KDD Cup 99	99.14 %	[51]
LR-DBN	KDD Cup 99	97,9 %	[52]
RNN	NSL-KDD	83,28%	[53]-[54]
LSTM	KDD Cup 99	93.85%	[55]- [56]-[57]
GRU	Netflow	84.15%	[58]
CNN	CTU-UNB Dataset, netflow	92%	[59]-[60]-[61]-[62]
ID-CNN	ISCX Dataset	97,3%	[63]
RAMDON FOREST	Cicids2017-NDSec1- Cse-CIC-IDS 2018-CIC-DDoS2019	99.9 %	[64]

Fuente: Y. Xin et al., "Machine learning and deep learning methods for cybersecurity," ieeexplore.ieee.org, 2018.

Fase 3: Establecer los lineamientos para la construcción de una arquitectura de las tecnologías emergentes IoT, técnicas de inteligencia artificial y tecnologías de monitoreo y almacenamiento de tráfico malicioso más utilizadas.

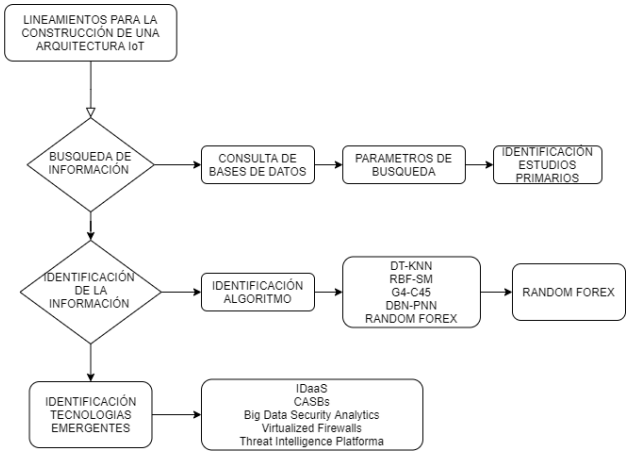

Fig. 3 Lineamientos establecidos en el presente estudio.
Fuente: Propia.

En esta fase se procede a establecer los lineamientos que se deben seguir para la construcción de una arquitectura de IoT, como se puede apreciar en la figura 3 se evidencia que la primera acción es realizar la búsqueda de información en donde se comprenden los pasos a seguir, entre ellos: consulta de bases de datos, seguido del establecimiento de parámetros de búsqueda y la identificación de estudios primarios, como segundo paso se establece la identificación de la información dentro de éste se establecen dos lineamientos que son: la identificación del algoritmo, que después de un listado de 26, se escogieron los 5 con valores más altos y de estos se seleccionó el algoritmo más indicado y finalmente se identifican de igual forma las tecnologías emergentes más adecuadas para el estudio, en este caso se logran identificar 6 tecnologías.

IV. RESULTADOS

Resultante de la fase 1, se tienen en total 109 documentos que después de ser filtrados con base a los parámetros anteriormente mencionados se tienen en total 55 documentos primarios, a partir de esto se establece la tabla III que indica el total de algoritmos que se lograron extraer de los diferentes estudios, es importante enmarcar dentro de este listado los 6 algoritmos con los porcentajes de precisión más altos, recordando que estos porcentajes son obtenidos a través de las pruebas y análisis que arrojan con cada Dataset, de modo que dentro de los 6 algoritmos más representativos están:

- PSO-SVM, 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, 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, este algoritmo se clasifica como un árbol de decisión en la que cada nodo interno representa una prueba en una propiedad, cada rama representa una salida de prueba y cada nodo hoja representa una categoría. La prueba de este algoritmo se dio en el Dataset KDD Cup 99 y arrojó 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, dando como resultante un 99,9% de precisión.
- RANDOM FOREX, se caracteriza por ser una integración 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.

Ahora bien, con 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, éste es 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.

La ciberseguridad actualmente tiene un panorama con muchas actualizaciones, pero se presentan algunas limitantes, entre ellas están: los volúmenes masivos de datos, la falta de análisis de estos y los diversos ataques son cada vez más frecuentes, complejos y puede limitarse en establecer una seguridad eficaz y apropiada. En virtud de lo anterior, es necesario generar sistemas que ofrezcan protección a los datos de diferentes entidades, pero para esto se debe insistir en la continua actualización en tecnologías emergentes asociadas a la ciberseguridad.

De este modo en la tabla II, se presenta un listado de las tecnologías emergentes que actualmente se han desarrollado y están en investigación para futuras aplicaciones, pero para este caso fueron las escogidas para el desarrollo del estudio, después de un análisis de la bibliografía filtrada, siendo así, se indica inicialmente a IDDaaS, esta tecnología se define como un conjunto de servicios de administración, identidad y acceso que se ofrecen a través de la red, tiene la capacidad de proporcionar diferentes servicios, entre ellos permitir que los usuarios puedan acceder a sus datos confidenciales de manera segura, uno de los beneficios es que tiene un manejo de bajo costo en mantenimiento, ocupa un mayor tiempo de actividad y no necesita hardware complejo, sus aplicaciones varían; sin embargo, se sugiere usar para conexiones seguras en recursos TI.

De igual forma se tiene CASBs, este tipo de tecnologías se definen como puntos especializados en políticas de seguridad, crean sistemas seguros entre consumidores de la red y los proveedores de servicios de éste, de ahí que cada vez se da más uso de este tipo de tecnologías, ya que se puede hacer frente a diferentes tipos de riesgos en los servicios de red.

Se tiene también a Big Data Security Analytics, son capaces de recopilar, almacenar y analizar grandes cantidades de datos, analizan los datos a través de varios algoritmos de correlación, para así detectar anomalías e identificar ataques maliciosos y reaccionar a tiempo frente amenazas. Una de las grandes ventajas que presenta Big Data Security Analytics es que su operación es en tiempo real y generan una especie de alarmas o alertas de seguridad, estas alarmas se clasifican de acuerdo con la gravedad del ataque, permitiendo así una detección y mitigación temprana.

Otra de las tecnologías emergentes es Virtualized Firewalls, se conoce como un elemento virtual que logra ofrecer opciones de seguridad, inspección y monitoreo de tráfico de red, el cual tiene y la supervisión de paquetes habituales que se proporcionan a través de un firewall de red físico, adoptando tecnología para la prevención de intrusos.

Finalmente, se tiene a la tecnología Threat Intelligence Platforms, se conoce como plataformas de inteligencia de amenazas, estas generalmente se dan uso para facilitar la gestión de la inteligencia de amenazas cibernéticas, tiene varias ventajas, entre las cuales están: la capacidad de agregar inteligencia de múltiples fuentes, de igual forma logra normalización y puntuación de riesgos de datos, también permite integrarse con sistemas de seguridad ya existentes y ofrece un análisis e intercambio de inteligencia sobre la amenaza detectada.

Por último, se establece que el algoritmo adecuado es RANDOM FOREX, esto apoyado de las seis tecnologías emergentes en mención, dado que se considera que todas tienen acción, uso e importancia dentro del estudio ejerciendo una función especifica para la gestión de las amenazas logrando disminuir el impacto a un incidente de seguridad a través de la articulación de cada una de ellas.

V. CONCLUSIONES

Con el creciente uso de dispositivos IoT, los datos y la información quedan expuestos y pueden representar una puerta de entrada para intrusos o robo de datos, por tal motivo la construcción de una arquitectura que identifique, gestione y mitigue a tiempo cualquier agente malicioso, es fundamental para crear sistemas y/o alternativas que permitan proteger los datos.

Es relevante, tener en cuenta que para el desarrollo de una arquitectura para dispositivos IoT, se deben considerar diferentes parámetros, entre ellos: la de un algoritmo inteligente, quien será el encargado de clasificar y determinar nuevos patrones de anomalías; así como también, tener a consideración la elección de las tecnologías emergentes adecuadas, éstas se deben estudiar de acuerdo a los objetivos principales del estudio, los datos a los cuales están enfocados y el nivel de ciberseguridad que se requiera aplicar.

AGRADECIMIENTOS

Agradecimientos a la Universidad del Cauca en especial a su grupo de investigación GTI y al grupo de investigación I+D en Informática de la Facultad de Ingeniería de la Institución Universitaria Colegio Mayor del Cauca, por el apoyo brindado para el desarrollo del proyecto.

REFERENCIAS

[1] F. Exequiel *et al.*, “Propuesta de un modelo de aplicación de IoT

y telemetría en los procesos de servicios de taller para empresas concesionarias automotrices," 2018. Accessed: Sep. 02, 2020. [Online]. Available: https://repositorio.esan.edu.pe/handle/20.500.12640/1391.

[2] J. Buil García, Á. López, and L. Madrid, "Análisis forense de un dataset industrial y propuesta de un estándar gráfico para los registros en la ciberseguridad," 2018. Accessed: Sep. 02, 2020. [Online]. Available: https://repositorio.comillas.edu/xmlui/handle/11531/23725.

[3] "IoT en ALC 2019: Tomando el pulso al Internet de las Cosas en América Latina y el Caribe | Publications," 2019. https://publications.iadb.org/publications/spanish/document/IoT_en_ALC_2019_Tomando_el_pulso_al_Internet_de_las_Cosas_en_América_Latina_y_el_Caribe_es.pdf (accessed Jul. 23, 2021).

[4] B. T.-I. T. de N. L. Web and U. 2007, "Introducción a la inteligencia artificial." Accessed: Mar. 08, 2021. [Online]. Available: http://www.cs.bham.ac.uk/~rmp/slide_book/slide.

[5] G. Veletsianos, "Emerging technologies in distance education," 2010. https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=George+Veletsianos+%282010%29+&btnG= (accessed Mar. 08, 2021).

[6] J. Salazar and Y. S. Silvestre, "INTERNET DE LAS COSAS," 2016. Accessed: Mar. 08, 2021. [Online]. Available: http://www.techpedia.eu.

[7] L. Chappel, "Wireshark Network Analysis.," 2012. https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q=Wireshark+Network+Analysis.+Chappel%2C+L.+%282012%29.+&btnG=#d=gs_cit&u=%2Fscholar%3Fq%3Dinfo%3AWjl3EUWT4xwJ%3Ascholar.google.com%2F%26output%3Dcite%26scirp%3D0%26hl%3Des (accessed Mar. 08, 2021).

[8] 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, doi: 10.1016/j.jnca.2020.102538.

[9] M. Aminu Lawal, R. Ahmed Shaikh, and S. Raheel Hassan, "An Anomaly Mitigation Framework for IoT Using Fog Computing," *mdpi.com*, 2020, doi: 10.3390/electronics9101565.

[10] 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, doi: 10.1007/s00521-020-04772-3.

[11] 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, doi: 10.1016/j.future.2019.09.002.

[12] F. J. Pino, M. Piattini, and G. H. Travassos, "Managing and developing distributed research projects in software engineering by means of action-research Gestión y desarrollo de proyectos de investigación distribuidos en ingeniería del software por medio de investigación-acción," 2013. Accessed: Mar. 09, 2021. [Online]. Available: https://revistas.udea.edu.co/index.php/ingenieria/article/download/17161/14849/0.

[13] T. P. Fowdur, B. N. Baulum, and Y. Beeharry, "Performance analysis of network traffic capture tools and machine learning algorithms for the classification of applications, states and anomalies," *Int. J. Inf. Technol.*, vol. 12, no. 3, pp. 805–824, Sep. 2020, doi: 10.1007/s41870-020-00458-0.

[14] P. P. Ray, "A survey of IoT cloud platforms," *Futur. Comput. Informatics J.*, vol. 1, no. 1–2, pp. 35–46, Dec. 2016, doi: 10.1016/j.fcij.2017.02.001.

[15] 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, doi: 10.1007/978-3-030-02686-8_10.

[16] A. Gómez-Cárdenas, X. Masip-Bruin, E. Marín-Tordera, and S. Kah-Vazadeh, "A Novel and Scalable Naming Strategy for IoT Scenarios," 2018. Accessed: Mar. 12, 2021. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-030-02686-8_10.

[17] Á. Alonso, F. Fernández, L. Marco, and J. Salvachúa, "IAACaaS: IoT Application-Scoped Access Control as a Service," *Futur. Internet*, vol. 9, no. 4, p. 64, Oct. 2017, doi: 10.3390/fi9040064.

[18] 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, doi: 10.1007/s11227-016-1634-x.

[19] 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, doi: 10.1145/3445969.3450427.

[20] A. R. Mathew and A. Al Hajj, "Secure Communications on IoT and Big Data," *Indian J. Sci. Technol.*, vol. 10, no. 11, 2017, doi: 10.17485/ijst/2017/v10i11/107974.

[21] 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, doi: 10.1109/COMST.2018.2862350.

[22] C. Lorenz *et al.*, "An SDN/NFV-Enabled Enterprise Network Architecture Offering Fine-Grained Security Policy Enforcement," *IEEE Commun. Mag.*, vol. 55, no. 3, pp. 217–223, Mar. 2017, doi: 10.1109/MCOM.2017.1600414CM.

[23] 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, doi: 10.3390/fi12060108.

[24] 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.

[25] Y. Xin *et al.*, "Machine learning and deep learning methods for cybersecurity," *ieeexplore.ieee.org*, 2018, Accessed: Mar. 11, 2021. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8359287/.

[26] 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/.

[27] 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.

[28] M. Shakil Pervez and D. M. Farid, "Feature selection and intrusion classification in NSL-KDD cup 99 dataset employing SVMs," *ieeexplore.ieee.org*, 2015, doi: 10.1109/SKIMA.2014.7083539.

[29] 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, doi: 10.1007/978-3-642-18333-1_12.

[30] 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/.

[31] … 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/.

[32] B. Rao and K. S. Science, "Fast kNN classifiers for network intrusion detection system," *sciresol.s3.us-east-2.amazonaws …*, 2017, doi: 10.17485/ijst/2017/v10i14/93690.

[33] 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).

[34] 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.

[35] W. Meng, W. Li, and L.-F. Kwok, "Design of intelligent KNN-based alarm filter using knowledge-based alert verification in intrusion detection Ž," *Networks*, vol. 8, no. 18, pp. 3883–3895, Dec. 2015, doi: 10.1002/sec.1307.

[36] 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).

[37] 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.

[38] 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, doi: 10.1007/978-3-319-63645-0_23.

[39] 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, doi: 10.1007/s10586-017-0971-8.

[40] 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/.

[41] 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, doi: 10.5120/ijca2015905983.

[42] C. Azad and V. Kumar Jha, "Computer Network and Information Security," *Comput. Netw. Inf. Secur.*, vol. 8, pp. 56–71, 2015, doi: 10.5815/ijcnis.2015.08.07.

[43] 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.

[44] 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.

[45] 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.

[46] 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/.

[47] 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.

[48] 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, doi: 10.1145/3171592.3171598.

[49] 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/.

[50] Q. Tan, W. Huang, and Q. Li, "An intrusion detection method based on DBN in ad hoc networks," Aug. 2016, pp. 477–485, doi: 10.1142/9789813140011_0056.

[51] 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/.

[52] 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/.

[53] 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/.

[54] N. R. RB Krishnan, "'An intellectual intrusion detection system model... - Google Académico," 2016. https://scholar.google.es/scholar?hl=es&as_sdt=0%2C5&q='An+intellectual+intrusion+detection+system+model+for+attacks+classification+using+RNN&btnG= (accessed Mar. 11, 2021).

[55] 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/.

[56] 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/.

[57] 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.

[58] 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, doi: 10.1145/3195106.3195117.

[59] 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/.

[60] 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, doi: 10.1007/978-3-319-50127-7_11.

[61] 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.

[62] 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, doi: 10.1109/ICOIN.2017.7899588.

[63] 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, doi: 10.1109/ISI.2017.8004872.

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

Juan José Caiza, Ingeniero en Informática y Especialista en Administración de la Información y en Bases de datos de la Institución Universitaria Colegio Mayor del Cauca, Colombia. Investigador en el área de Ciberseguridad e integrante del Semillero Beta Bit. Co-autor de varios libros y ponente en conferencias tanto a nivel nacional e internacional.

Katerine Márceles Villalba, Ingeniero de Sistemas de la Fundación Universitaria San Martín – sede Caribe, Colombia, Magister en Seguridad Informática de la Universidad Internacional de la Rioja, España. Investigador en el área de Ciberseguridad, Coordinador del Semillero Beta Bit de la Institución Universitaria Colegio Mayor del Cauca. Co-autor de varios libros y ponente en conferencias tanto a nivel nacional e internacional.

Siler Amador Donado, Ingeniero de Sistemas de la Universidad del Norte, Colombia, Magister en Seguridad Informática de la Universidad Internacional de la Rioja, España. Investigador en el área de Ciberseguridad, Coordinador del Semillero Security, Encryption & Cybersecurity de la Universidad del Cauca, Colombia. Co-autor de varios libros y ponente en conferencias tanto a nivel nacional e internacional.