UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA DE COMPUTACION

Trabajo de titulación previo a la obtención del título de:
Ingeniero en Ciencias de la Computación

TEMA:
ESTADO DE ARTE DE PUBLICACIONES SOBRE CIBERATAQUES A DISPOSITIVOS DE CIUDADES INTELIGENTES

AUTORES:
JERSSON ALEXANDER IZA LEMA
STHEFANY ALEXANDRA SÁNCHEZ BEDÓN

TUTOR:
JOSE LUIS AGUAYO MORALES

Quito - Ecuador
2022

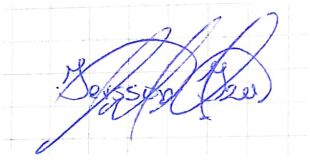
CERTIFICADO DE RESPONSABILIDAD Y AUTORíA DEL TRABAJO DE TITULACIÓN

Nosotros, Jersson Alexander Iza Lema, con documento de identificación N° 1724486392 y Sthefany Alexandra Sánchez Bedón, con documento de identificación N° 1724928963; manifestamos que:

Somos los autores y responsables del presente trabajo;y, autorizamos a que sin fines de lucro la Universidad Politécnica Salesiana pueda usar, difundir, reproducir o publicar de manera total o parcial el presente trabajo de titulación.

Quito, 14 de septiembre del año 2022

Atentamente,



Jersson Alexander Iza Lema
1724486392

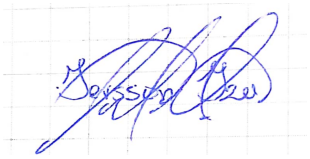
Sthefany Alexandra Sánchez Bedón
1724928963

CERTIFICADO DE CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE TITULACIÓN A LA UNIVERSIDAD POLITÉCNICA SALESIANA

Nosotros, Jersson Alexander Iza Lema, con documento de identificación N° 1724486392 y Sthefany Alexandra Sánchez Bedón, con documento de identificación N° 1724928963, expresamos nuestra voluntad y por medio del presente documento cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del Artículo Académico intitulado: "Estado de Arte de Publicaciones Sobre Ciberataques a Dispositivos de Ciudades Inteligentes.", el cual ha sio desarrollado para optar por el título de Ingenieros en Ciencias de la Computación en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia con lo manifestado, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

Quito, 14 de septiembre del año 2022

Atentamente,



Jersson Alexander Iza Lema
1724486392

Sthefany Alexandra Sánchez Bedón
1724928963

CERTIFICADO DE DIRECCIÓN DEL TRABAJO DE TITULACIÓN

Yo, Jose Luis Aguayo Morales con documento de identificación N° 1709562597, docente de la Universidad Politécnica Salesiana, declaro que bajo mi autoría fue desarrollado el trabajo de titulación, con el tema: ”Estado de arte de Publicaciones sobre Ciberataques a Dispositivos de Ciudades Inteligentes”, realizado por Jersson Alexander Iza Lema con documento de identificación N° 1724486392 y Sthefany Alexandra Sánchez Bedón con documento de identificación N° 1724928963, obteniendo como resultado final el trabajo de titulación bajo la opción de Artículo Académico que cumple con todos los requisitos determinados por la Universidad Politécnica Salesiana.

Atentamente,

Quito, 14 de septiembre del año 2022

.....

Ing. Jose Luis Aguayo Morales, MSc
1709562597

Estado de arte de Publicaciones sobre Ciberataques a Dispositivos de Ciudades Inteligentes

*State of the Art publications on Cyberattacks on Smart City Devices

1st Jersson Alexander Iza Lema
jizal2@est.ups.edu.ec

2nd Sthefany Alexandra Sánchez Bedon
ssanchezb3@est.ups.edu.ec

3rd José Luis Aguayo Morales
jaguayo@ups.edu.ec

***Resumen*—El término "ciudad inteligente" existe desde hace un tiempo, pero ha llegado a ser más habitual últimamente . La idea es que al utilizar la tecnología en dispositivos para hacer que las ciudades sean más habitables, sostenibles y eficientes, ofreciendo mejores servicios a sus residentes y convertirse en mejores lugares para trabajar. Pero a medida que más ciudades invierten en estos proyectos, también se exponen a ataques cibernéticos que podrían destruir sistemas de infraestructura críticos, como redes eléctricas, tráfico, salud inteligente y seguridad ciudadana. Para ejecutar este estado de arte se va a realizar (SMap) mapeo sistemático y (SLRev) revisión de lectura sistemática sobre los ciberataques que constan en publicaciones científicas contra las ciudades inteligentes en su privacidad de los datos. SLRev nos ayudó para conseguir la taxonomía de ciberataques que vulneran a los dispositivos los cuales se dividen en CIA, dando como fruto los ataques más relvenates para cada clasificación. En primer lugar, el ciberataque que vulnera la confidencialidad es Spoofing con un porcentaje de 16.22%, en segundo lugar, el ciberataque que vulnera la Integridad es: Inyección de datos con un porcentaje de 42.31% y en tercer lugar el ciberataque que vulnera la disponibilidad es DDoS con un porcentaje de 42.86%. Con esto se llega a la conclusión que un ciberataque es una acción deliberada para interrumpir, negar, degradar o destruir datos y/o información, puede estar dirigido a cualquier tipo de organización y se los puede detectar mediante diversas técnicas de Inteligencia Artificial.**

***Index Terms*—Ciberataque, ciudad inteligente, dispositivos, técnicas.**

***Resumen*—The term "smart city" is means that by using technology and devices transform the cities making more liveable, sustainable and efficient; to give better services to their residents and become better places to live and work. However, when more cities invest in these projects, they expose themselves to critical infrastructure cyberattacks, such as power systems, traffic, health services, etc. This investigation executed a state of the art using: (SMap) systematic mapping and (SLRev) systematic reading review about cyberattacks that appear in scientific publications against smart cities or their data privacy. SLRev helped to obtain the taxonomy of cyberattacks that compromise their confidentiality, integrity or availability. The research results show the most relevant attacks for each classification, first is revealed that cyberattack that violates confidentiality is spoofing with a 16.22%; second is the cyber-attack againts the Integrity that is data injection with a 42.31%; and third is the attack to violate availability is DDoS with a 42.86%. Finally, a cyberattack is a deliberate action to interrupt, deny, degrade or destroy data and/or the information that it can directed at any organization but it may detected through various Artificial Intelligence Techniques.**

***Index Terms*—Cyber attack, smart city, devices, techniques.**

I. Introducción

Hoy en día, varias ciudades han sido clasificadas como ciudades inteligentes las cuales se han construido para ofrecer un mejor desarrollo de nivel de vida alto a sus ciudadanos, utilizando tecnología digital y datos para realizar mejoras en su transporte, energía y otras infraestructuras, según [1] mantener las capacidades de sostenibilidad y resiliencia requiere que la ciudad inteligente se adapte a los cambios generados por factores sociales, políticos, ambientales y naturales también debe brindar seguridad tanto a sus ciudadanos como a las infraestructuras críticas que soportan la provisión de servicios críticos como energía, agua, comunicaciones, educación, salud, entre otros.

Sin embargo, los dispositivos que integran las ciudades inteligentes han estado expuestos a varios ciberataques los cuales se están volviendo gradualmente más inteligentes. En consecuencia, el análisis de amenazas cibernéticas está llamando la atención, al analizar e interpretar la tendencia del ataque mediante el compendio de una cantidad grande de información sobre ataques cibernéticos y la realización de su análisis.

Para obtener un estado de arte de las publicaciones de ciberataques a dispositivos de las ciudades inteligentes, teniendo en cuenta su enfoque se recopilaron investigaciones realizadas desde el 2017 hasta el presente año; se llevó a cabo un (SMap) Mapeo Sistemático que se dividió en 3 ciclos y se aplicó (SLRev) Revisión sistemática de la Literatura. Después de identificar cuidadosamente los estudios relacionados. Las contribuciones que se llevaron a cabo en esta investigación son: 1) Realizar Mapeo y Revisión Sistemática basados en clasificación de ciberataques en dispositivos de ciudades inteligentes. 2) Este documento examina el estudio de ciberataques que agreden a la confiabilidad, integridad y disponibilidad de los sistemas (CIA) y han sido detectados con un enfoque basado en técnicas de inteligencia artificial. 3) Determinar los ciberataques más frecuentes que han sido detectados en los dispositivos.

II. Metodología

SMap. es una herramienta de ideas y contextualización, se basa en la determinación, examinación y clasificación de métodos para analizar ataques cibernéticos en dispositivos de ciudades inteligentes, SLRev. permite programar, ejecutar y

producir evaluaciones sistemáticas para conseguir investigaciones ideales del tema en estudio dentro del periodo 2017 - 2022. [2]

Una ciudad inteligente se encuentra compuesta por tecnologías de información y comunicación, promoviendo e implementando prácticas para su desarrollo lo cual lo hace vulnerables a los ciberataques que tienen como propósito quebrantar la CIA de los datos lo cual vienen dado debido a la ciberdelincuencia.

Al realizar este estado de arte se efectuó la metodología SMap. y SLRev., que se constituyen en los siguientes ciclos: Ciclo1 se basa en los criterios de selección donde se define objetivos y alcance. Ciclo 2 se ejecutó la inspección y extracción de los esenciales argumentos encontrados en cada investigación. Ciclo 3 sigue las normas de SMap. y SLRev. Para la clasificación de los estudios seleccionados se realizaron:

A. Ciclo 1

Para obtener las investigaciones relacionadas con los ciberataques ocurridos en dispositivos de ciudades inteligentes, se adaptó de acuerdo a la esrategia PICOC la explicación de los componentes de indagación (ver tabla I).

Población (P): ¿Quién?	Dispositivos
Intervención (I): ¿Qué o Cómo?	Ciberataques a ciudades inteligentes
Comparación (C): ¿Comparado con qué?	Artículos que presentan los ciberataques a ciudades inteligentes
Resultado (O): ¿Qué se quiere lograr/mejorar?	btener información concreta, compilada y verificada para advertir los ciberataques a las ciudades inteligentes.
Contexto (C): ¿Bajo qué circunstancias y que tipo de organización?	Examinar las investigaciones que traten sobre ciberataques ocurridos a dispositivos de las ciudades inteligentes

Tabla I: Implementación método PICOC

Después de desarrollar este método se identificaron términos que serán de ayuda para establecer la cadena de búsqueda que se visualizan en la tabla II. Se emplearon caracteres booleanos, estos son: “AND” y “OR”, de la siguiente manera: (“Cyberattacks OR Malicius software OR Malicius Devices” AND “Devices OR Machine” AND “Smart Cities OR Smart Buildings OR Intelligent building”).

Términos	**Análogos**
Smart Cities	Smart Buildings, Intelligent building, domotic, public utilities
CyberAttacks	Malicius Software, Malicius Devices,Dos DDos
Devices	Devices, domotic, IoT devices, controllers, supply chain

Tabla II: Bocablos para la composición de cadena de indagación

Criterios de estudios: SMap. Y SLRev contienen dos tipos de criterios para recolectar papers de investigación más relevantes que se enumeran a posteriori:

- Criterios de exclusión: Excluir todas las investigaciones publicadas que se encuentren en español, que tengan menos de cinco páginas, duplicados o relacionados con cualquier otro ataque cibernético que no se haya llevado a cabo en una ciudad inteligente.
- Criterios de inclusión: Durante la búsqueda de los cuatro repositorios se establecieron varios criterios: artículos incluidos en el título y selección de palabras claves en el resumen, se buscó evidencia empírica sobre los ciberataques a dispositivos de ciudades inteligentes.

B. Ciclo 2

1) Preguntas de Investigación: El propósito fundamental de este análisis fue llevar a cabo el desarrollo del estado del arte de ciberataques a dispositivos de ciudades inteligentes por lo que se definieron preguntas de investigación para SMap. y SLRev. las cuales se indican más adelante:
   - SMP1 ¿Qué técnicas existentes destacan en la detección de ciberataques a los dispositivos en ciudades inteligentes?
   - SMP2 ¿Cuáles son los dispositivos que han recibido un ciberataque con mayor frecuencia en las ciudades inteligentes?
   - SLRP1 ¿Cuáles son los servicios vulnerables a un ciberataque que forman parte de la ciudad inteligente?
   - SLRP2 ¿Cuáles son los principales ataques publicados de disponibilidad, integridad o confidencialidad a dispositivos en las ciudades inteligentes?
   - SLRP3 ¿Que ciberataques han recibido las capas en la infraestructura de ciudades inteligentes?
   - SLRP4 ¿Cuál es el nivel de amenaza y taxonomía de usuarios en las ciudades inteligentes?
2) Plan de búsqueda. Las secuencias de indagación fueron aplicadas en cuatro bases de datos preseleccionados (ver Tabla III) para garantizar que hubiera gran cantidad de publicaciones disponibles para realizar estudios de SMap. y SLRev. Al efectuar F1 se almacenaron 1.500 publicaciones. Para el banco de datos ScienceDirect, IEEE, Springer y ACM se tomó en cuenta los últimos 5 años.
   En F2, utilizando Mendeley, la información se depuró basándose en palabras clave y resúmenes, reduciendo así el número de estudios a 1000 estudios.Los artículos finales se obtuvieron en el tercer filtro los cuales fueron leídos utilizando criterios de inclusión y exclusión para terminar seleccionando 60 papers.

Tabla III: Cadenas de indagación

BASE DE DATOS	CADENA	Tipo Artículo	F1	F2	F3
Science Direct	”Cyberattacks OR Threats” AND ”Appliances OR Supply Chain” AND” Smart cities OR Domotic”	Revistas y Conferencia	1000	690	37
ACM	“Ciberattacks OR Malicius software OR Malicius Devices” AND “Devices OR Invention OR Machine” AND “Smart Cities OR Smart Buildings OR Intelligent building”	Revistas Y Conferencias	155	90	8
SPRINGER	Dod DDoS OR malware” AND “Devices OR IoT Devices” AND “Smart Building OR Public Utilities”	Revistas	145	70	1
IEEE	“Malicius Software OR Malicius Devices” AND “Devices OR domotic” AND “Intelligent building OR Smart Cities”	Revistas y Conferencias	200	150	14

C. Ciclo 3

Mediante la obtención de datos se logró esbozar la información de los estudios analizados anteriormente, gracias al SLRev. se pudo plasmar de manera conceptual la clasificación de los ciberataques a dispositivos de ciudades inteligentes (ver figura 1).

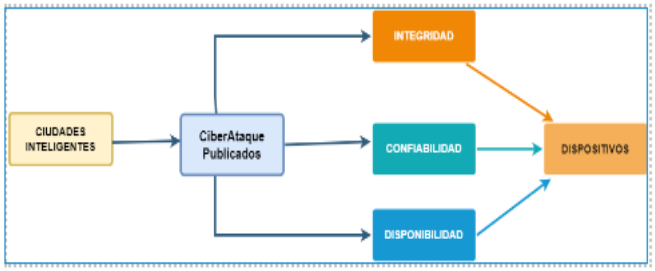


Fig. 1: Esquema de un ciberataque a dispositivos de una ciudad inteligente.

a) Ciudades Inteligentes: Las ciudades inteligentes deben utilizar todas las tecnologías que son necesarias para su desarrollo, a saber: Computación en la nube, sistemas de información geográfica espacial, big data e Internet de las cosas etc [3]

De acuerdo con el proceso de SMap y SLRev se extrajo información de manera contundente para el desarrollo del boceto de arquitectura de una ciudad inteligente (ver figura 2).

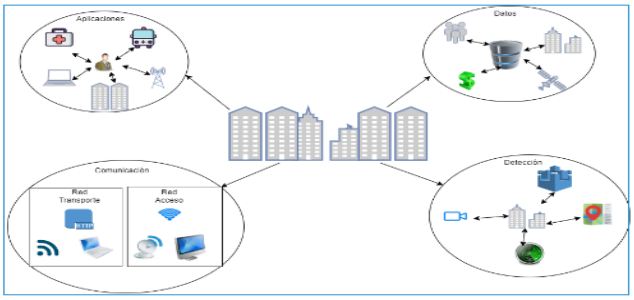


Fig. 2: Boceto de arquitectura de Smart City.

Se conoce como ciudad inteligente al conjunto de tecnologías como dispositivos y redes de comunicación [4] que a su vez se clasifican en 4 capas: capa de aplicación, datos, comunicaciones y detección (ver figura 2), por lo que si llega a existir alguna falla en la arquitectura se generará una gran inseguridad que afectará a los ciudadanos y esto a su vez propagará el aumento de ciberataques [1].

b) Ciberataque: Un ciberataque es un conjunto de recursos de ataque que pretende vulnerar la información almacenada en los dispositivos físicos y lógicos (ver figura 3). En otras palabras, el análisis de ciberataques implica mapear los recursos de infracción y analizar la combinación de manera efectiva. Luego se realiza un análisis a los ataques y se plantean las estrategias e intenciones de los atacantes [4]. Para propagar código malicioso, es necesario que un atacante asegure los recursos infractores (código malicioso, sitio distribuido, sitio de explotación, código de explotación, sitio de inicio, sitio de ataque, vulnerabilidad, etc.)

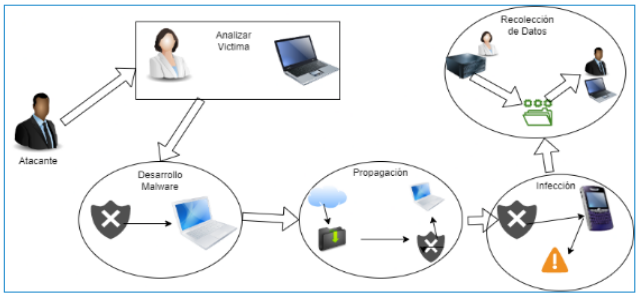


Fig. 3: Boceto de CiberAtaque.

c) Ataque en ciudades inteligentes. : Las ciudades inteligentes pueden compensar muchos de los problemas que provocan malestar entre los ciudadanos al conocer la calidad del aire, la congestión del tráfico, servicios médicos y del gobierno, todos estos servicios padecerán algún daño grave debido a los ciberataques que evolucionan día a día.

Según [5] los ataques de spear phishing aumentaron 55% años tras año en 2015, pero la cantidad de víctimas por correo de ataque se redujo en un 39%. Incluso en el año 2016 se encontraba en auge el ciber ataque conocido como ransonware el cual solo se pudo detectar y detener a 247 millones en la mitad de dicho año.

Se deben considerar los objetivos primordiales de la seguridad que son Confidencialidad, Integridad y Disponibilidad (CIA) ya que es un punto de partida

para contrarrestar el malware en cada dispositivo, por lo que se realizó una clasificación de ataques para cada uno de estos principios.

d) Ataque de Confidencialidad.: En [6] estos ataques han sido diseñados para vulnerar, robar, extraer y hurtar información de tipo personal, los nombres, los números telefónicos, contraseñas, correo electrónico, cuentas bancarias, etc. Son algunos ejemplos de información personal, cumpliendo con la finalidad de negociar con los mismos, en estos casos el atacante pretende aprovechar los datos que incluso se llegan a vender en las profundidades del internet.

Los ejemplos de ataques de confidencialidad integran violaciones de datos causadas por delincuentes, personas internas que entran o comparten información de forma inapropiada, repartición accidental de información confidencial. La tabla IV indica los ataques de confidencialidad recopilados los cuales han sido etiquetados para mayor comprensión.

N	Ataque de Confidencialidad	Referencia
C1	Acceso no autorizado	[7], [8]
C2	Amenaza avanzada persistente APT	[9]
C3	Ataque drive-by	[10]
C4	Ataques de contraseña	[11]
C5	Ataques de tráfico	[12], [13]
C6	Ataques de control de acceso	[14]
C7	Ataques en dominio	[3]
C8	Backdoring	[15], [11]
C9	Scan	[16], [17], [18], [19]
C10	Ataques Nodos Maliciosos	[14], [20], [21]
C11	Fuga de información	[22]
C13	Ataque man-in-the-middle	[10], [23], [24]
C14	Mapeo por cable e inalámbrico	[25]
C15	Phishing	[26], [14], [27], [23]
C16	Spoofing	[3], [7], [14], [28], [29], [30]
C17	Troyanos	[31], [32], [33]

Tabla IV: Ejemplos de Ataques de Confidencialidad

e) Ataque de Integridad.: En [6] Integridad significa que los datos y la información se mantienen para que no sean modificados por personas no autorizadas. Este es un componente fundamental de la limpieza, fiabilidad y exactitud de la información.

Para proteger la inquisición de lo datos, los procedimientos más simples son hacer una réplica de estabilidad de sus datos, utilizar controles de ingreso, monitorear su registro de auditoría y cifrar sus datos.

Los ejemplos de ataques a la integridad son ataques de fraude por correo electrónico (que comprometen la integridad de las comunicaciones), fraude financiero, inclusive ataques que perjudicaron la totalidad de datos del control industrial y provocaron perjuicios físicos.

La tabla V indica los ataques que vulneran la integridad de los dispositivos en las ciudades inteligentes.

N	Ataque de Integridad	Referencia
I1	Anomalías e intrusos	[12], [34], [33]
I2	Ataque de acceso remoto	[35], [31], [36]
I3	Ataque de usuario	[37], [38], [39]
I4	Sabotaje de datos	[9]
I5	Inyección de datos falsos	[3], [34], [40], [22], [41], [11], [42], [43], [44], [45], [46]
I6	Ataques de seguridad física	[34], [45], [47]
I7	Scripts Maliciosos	[26]
I8	Sybil attack	[4]

Tabla V: Ejemplos de Ataques de Integridad

f) Ataque de Disponibilidad.: En [6] menciona que los sistemas y los datos permanecen accesibles para los individuos una vez que los requieren en cualquier situación, cortes de energía o desastres naturales. Sin disponibilidad, su comercio puede verse perjudicado de manera negativa.

Para asegurar la disponibilidad, su organización puede usar varias aplicaciones. Estos pueden desarrollarse rápidamente para atacar al sistema una vez que este se descomponga.

Los ejemplos de ataques a la disponibilidad integran ataques de denegación de servicio, ataques que cifra los datos y archivos del sistema para que no sean disponibles para usuarios legítimos, inclusive ataques que tienen la posibilidad de interrumpir las operaciones comerciales.

En la Tabla VI se visualiza los ataques que dañan la disponibilidad.

N	Ataque de Disponibilidad	Referencia
D1	Ataque de canal lateral	[40]
D2	Ataques de evasión	[3]
D3	Ataques de sumidero	[40]
D4	Ataques on-off	[4], [42]
D5	Ataques volumétricos	[48]
D6	Botnet	[12], [49], [50], [51], [52], [37], [13], [53], [54]
D7	DDoS	[12], [34], [40], [7], [22], [49], [50], [51], [35], [38], [41], [16], [55], [43], [56], [57], [58], [59]
D8	Firmware	[4]
D9	Mirai	[49], [59]
D10	Ramsomware	[3], [13], [42], [53]
D11	Ping flood	[19]
D12	Spam	[24], [46], [60]

Tabla VI: Ejemplos de Ataques de Disponibilidad

g) Técnicas de detección de ataques.: Una técnica o enfoque está conformado por diferentes disciplinas, como ingeniería, arquitectura, diseño urbano y economía, para planear, diseñar, llevar a cabo y desplegar una solución inteligente para una labor subyacente. En [3] se dice que las técnicas de IA (inteligencia artificial) han demostrado ser bastante efectivas para obtener información de los datos recopilados por medio de diferentes dispositivos para regir y usar los recursos de forma más eficiente, en general incluye técnicas y algoritmos capaces de aprender de los datos (es mencionar, ciencia de

datos, aprendizaje estadístico, aprendizaje automático, aprendizaje profundo) o sistemas capaces de hacer labores como la percepción, el entendimiento, inferencia (es mencionar, sistemas profesionales, modelos gráficos probabilísticos, redes bayesianas).

En las publicaciones estudiadas se han hallado varias técnicas con las cuales ha sido posible la detección de varios ciberataques que se han dado a los diferentes dispositivos que conforma las ciudades inteligentes como se detalla en la Tabla VII.

N	Técnica	Referencia
T1	Algoritmo de suma acumulativa (CUSUM)	[46]
T2	Árbol de decisiones	[12], [3], [50], [28], [25], [19]
T3	AttriSel-kmodes	[9]
T4	Big data	[4], [3]
T5	Blockchain	[34], [38]
T6	Cloud computing	[4], [31], [15], [61], [24], [58], [60]
T7	Conmutación ADT	[26]
T8	Conmutadores sdn	[22], [7]
T9	Criptografía	[40], [7], [41], [46], [36]
T10	Enrutamiento Ad-hoc (ADOV)	[41], [14], [20], [28], [21]
T11	Grafos	[27], [40]
T12	K-Nearest Neighbor	[12], [3], [40], [49], [38], [31], [32], [13], [53], [48], [19], [47]
T13	Lógica difusa	[28], [30]
T14	Lyapunov	[55], [23]
T15	Minimización de entropía geométrica (GEM)	[33]
T16	Naïve Bayes (NB)	[12], [33], [42], [53], [29], [27], [44], [39]
T17	Redes neuronales	[12], [3], [10], [51], [11], [14], [20], [19], [39], [59]
T18	Regresión logística	[49], [37]
T19	Semi-supervised Fuzzy C-means	[35], [53], [46]
T20	Simulación	[10], [37], [32], [11], [42], [48], [14], [43], [62]
T21	Soporte vectorial	[49], [50], [52], [53], [23], [57], [58]

Tabla VII: Ejemplos de Técnicas

h) Dispositivos: Un administrador de la ciudad inteligente asegura los dispositivos que se encuentran en conectividad con la red y protege de otras máquinas infectadas. Un dispositivo IoT que verifica e informa de vez en cuando sobre la temperatura, la humedad y la atmósfera del clima. De acuerdo con [9] los sistemas inteligentes están transformando las redes de energía, las cadenas de suministro y la gestión del agua. Los sistemas de salud inteligentes pueden reducir drásticamente el costo de la terapia. Los sistemas alimentarios inteligentes están utilizando tecnología de identificación por radiofrecuencia para rastrear la carne y las aves desde la granja a través de la cadena de suministro hasta los estantes de las tiendas.

En la tabla VIII se puede observar con detalle los dispositivos que han sido afectados por los diferentes ciberataques detectados.

N	Dispositivo	Ataque	Referencia
1	Acceso remoto a energía	(I5)	[19]
2	Actuadores	(C2),(D7),(C15)	[9], [23], [25]
3	Cámaras ip	(D6),(C15),(C13)	[49], [51], [52], [56], [25], [59]
4	Control de acceso	(D7),(C16)	[58], [47]
5	Control de industria	(D7),(I5),(I7)	[10], [11], [48]
6	Dispositivos de salud	(C13),(D8), (C15), (C6)	[10], [55], [48], [28]
7	Dispositivos GPS	(I5),(D7),(I1),(I2)	[34], [35], [31], [41], [33]
8	Dispositivos GSM/3G/4G	(D1),(I8),(I2),(C17), (C9),(I3)	[4], [40], [35], [31], [53], [46]
9	Dispositivos móviles	(D7),(C16),(C13), (D12), (I5)	[40], [14], [43], [27], [57], [39], [47]
10	DNS	(D7),(D6),(C4)	[49], [50], [42], [53], [29]
11	Enrutadores domésticos	(D9),(I5),(C14)	[49], [29], [17]
12	Enrutadores empresariales	(D9)	[62]
13	ISP	(D11)	[24]
14	Nodos	(I6),(D4),(C10), (D3)	[34], [4], [28], [43]
15	nube móvil	(C15),(C9),(D7)	[20], [19], [45]
16	pozos de agua	(C1)	[7]
17	redes	(I1),(C5),(D7), (D10), (C10)	[12], [34], [51], [16], [61], [36]
18	RFID	(C16),(I5),(C11), (I3),(C8),(C16), (C1),(C9),(I2)	[7], [22], [37], [15], [9], [63], [24], [60]
19	sensores	(C7),(D10),(I5), (D2),(C1),(D7), (I4),(C17),(C8)	[3], [7], [50], [38], [9], [33], [11]
20	señalización	(D7)	[26]
21	sistema hidráulico	(C17),(D10),(D6), (D5),(C9)	[32], [13], [61], [8], [18]
22	sistemas de iluminación	(D4),(I5),(D7)	[16], [64], [62]
23	sistemas de trafico	(C3),(D6),(D7)	[10], [13], [41]
24	vehículos	(I5),(D6),(I3),(C5)	[40], [37], [38], [13], [16]
25	vehículos aéreos	(D7)	[22]
26	videocámaras	(I6),(D12)	[39], [21], [54]

Tabla VIII: Dispositivos Atacados

III. Resultados y Discusión

A. SMP1 ¿Qué técnicas existentes destacan en la detección de ciberataques a los dispositivos en ciudades inteligentes?

Detectar la ciruculación de ataques cibernéticos es primordial. Teniendo en cuenta [12] un patron de caracterización de la circulación de, intrusiones, ataques cibernéticos y anomalías usando algoritmos de IA ya que se fundamentan en conjuntos de datos que se utiliza extensamente a partir de la última década y es notable que ML puede funcionar realmente bien para la detección de ataques cibernéticos.

Como se visualiza en figura IV, al realizar la descomposición, las técnicas más relevantes para la exploración de un ciberataque destacan 3 las cuales son: K-Nearest Neighbor (T12), Redes neuronales (T17) y Simulación (T20).

K-Nearest Neighbor (T12): Conocido como KNN o k-NN, es un clasificador de aprendizaje supervisado no paramétrico ya que no hace suposiciones sobre el reparto de datos subyacente únicamente aspira decidir a qué conjunto pertenece un punto de datos, según [65] este algoritmo usa la proximidad

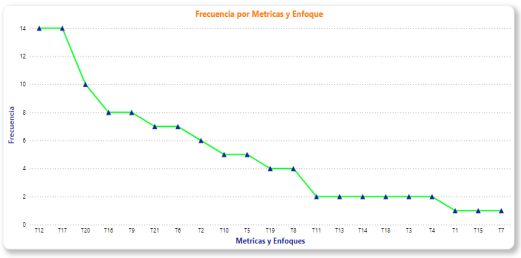


Fig. 4: Frecuencia Metricas.

para hacer clasificaciones o predicciones sobre la agrupación de un punto de datos personal y se basa en datos de ingreso etiquetados para aprender una funcionalidad que crea un resultado apropiado una vez que se le brindan nuevos datos no etiquetados.

Redes neuronales (T17): Son programadas en software. La primera capa de neuronas recibirá entradas como imágenes, clip de video, ruido, etc. En [66] indica que las redes neuronales o sus conjuntos tienen la posibilidad de usar para abordar de forma inteligente diferentes inconvenientes de ciberseguridad, incluida la detección de intrusiones, el estudio de malware, la investigación de amenazas de estabilidad, la predicción de ciberataques o anomalías.

Simulación (T20): En [67] expresa que las técnicas de simulación son abstracciones deliberadas de los sistemas físicos para explorar cómo la compleja interrelación entre los sistemas humanos, sociales, de programa y de hardware podría crear vulnerabilidad o resiliencia, otorgan un medio para analizar colaboraciones y cambios complicados dentro del sistema en todo el tiempo, incluida la predominación de los actores sociales.

B. SMP2 ¿Cuáles son los dispositivos que han recibido un ciberataque con mayor frecuencia en las ciudades inteligentes?

En la investigación realizada se pudieron descubrir 26 dispositivos los cuales han sufrido algún tipo de ciberataque (ver tabla VIII), contemplando los datos se pudieron evidenciar 4 dispositivos que enfatizan en este análisis como se ve en la Figura 6 estos son: Redes, sensores, RFID y dispositivos móviles. Cada uno de ellos ha vulnerado con diferentes malwares, que se explicarán a continuación:

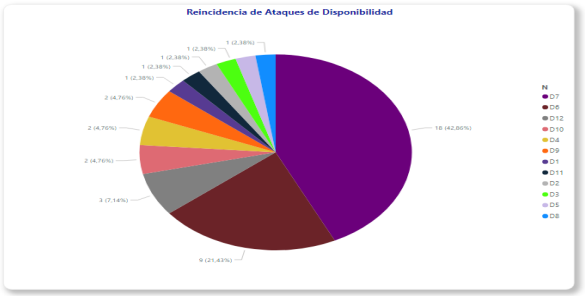


Fig. 5: Reincidencia Dispositivos.

Redes: Estos dispositivos están diseñados para realizar tareas de manera específica para la comunicación, diseño, interacción y seguridad de la red informática. En [68] se dice que estos dispositivos se deben monitorear cuidadosamente, para que puedan detectar de manera eficaz ataques cibernéticos. En este estudio se pudo conocer que los ataques que han recibido estos dispositivos son: I1 los cuales han sido detectados con 2 diferentes técnicas T16 y T5, C5 detectado con la técnica T12, C10 con técnicas T2 y T10, D6 con T2, D7 utilizando la técnica T17 y D10 con T16.

Sensores: Son dispositivos que adquieren y responden a algún tipo de entrada específico del entorno donde se encuentran, estas entradas pueden ser: movimiento, luz, calor, etc. En las publicaciones estudiadas se identificó que este tipo de dispositivos han sufrido ciberataques como: C1 utilizando T9, D9 con T2, C7, C8 y D10 con T17, ataques D7 donde se utilizaron dos tipos de técnicas para su detección que son T5 y T21, I5 con la técnica T12, I4 con T4 y C17 con T16.

RFID: Es un dispositivo diseñado para brindar comunicación de manera inalámbrica a través de los espectros electromagnéticos para facilitar la detección de objetos, persona y animales. En el análisis de los datos se logró distinguir que estos dispositivos se han visto vulnerables a los ciberataques de igual manera cada uno de estas vulnerabilidades han sido detectadas por los métodos de ML, desglosamos cada ataque con el método utilizado para su detección: C16 e I2 utilizando T9, I5 y C11 utilizando T8, I3 utilizando T18, C8 utilizando T6, C16 utilizando T3, C1 utilizando T20, C9 utilizando T12.

Dispositivos Móviles: Hace referencia de manera general a diversos computadores portátiles, celulares, etc. Se encuentran diseñados para facilitar la movilidad del usuario. Su funcionalidad es permitir la conexión a cualquier red en la que el usuario se encuentre cerca, debido a que se encuentra en auge han sido objetos sin duda de los ciberdelincuentes, gracias al reconocimiento de los datos realizados en la investigación se constató que existen diferentes ciberataques y cada uno de estos con el método de detección como: D7 utilizando T9, en varios casos se encontró que para un ataque fuera descubierto se utilizaron diferentes métodos como es el caso de C16 utilizando T17, T13 y T16, C13 utilizando T21, D12 utilizando T6, I5 utilizando T17.

C. SLRP1 ¿Cuáles son los servicios vulnerables a un ciberataque que forman parte de la ciudad inteligente?

La deficiencia de la arquitectura en una ciudad inteligente puede colocar en peligro a los datos de los habitantes y exponer la ciudad inteligente al aumento de ciberataques. Se detallan las vulnerabilidades que pueden presentar las aplicaciones de la ciudad inteligente y así recibir ataques cibernéticos.

*Transporte Inteligente:*Este servicio facilita movilidad, reducción del tráfico vehicular, y disminución de la contaminación en caso de que exista un ciberataque al servicio puede afectar a la sociedad y economía de la ciudad debido a que el ciberdelincuente puede modificar señales de tránsito

e interrumpir el servicio eléctrico y así inmovilizar a los ciudadanos.

Salud Inteligente: Es uno de los servicios que más impacto tiene en los habitantes ya que estos serían los más afectados, de modo que su privacidad se vería expuesta si ocurre un ciber-ataque puesto que tienen acceso directo a toda la información del paciente y de esta manera podrían utilizarla de manera maligna y lucrativa.

Seguridad Ciudadana: Los ciberataques a este servicio son basados en delitos, atracos y vandalismo, porque se tiene acceso a las cámaras de seguridad de toda la ciudad, a su vez causa preocupación en aspectos de la privacidad de los ciudadanos dado que se pueden obtener todos los datos personales relevantes mediante sus dispositivos móviles.

Hogares Inteligentes: Este servicio afecta principalmente a una familia en particular ya que son los que se verán perjudicados en caso de pasar por un ciberataque, el ciberdelincuente puede utilizar un solo dispositivo para tener el control total de la información almacenada dentro del hogar, invadiendo su privacidad y hurtando información valiosa para los habitantes.

D. SLRP2 ¿Cuáles son los principales ataques publicados de disponibilidad, integridad o confidencialidad a dispositivos en las ciudades inteligentes?

En la indagación de los ataques a la Disponibilidad del estudio realizado se pudo constatar que existen varios ataques (ver tabla VI), los que se encuentran en auge son 2: DDoS (D7), Botnet (D6); (Ver figura 6).

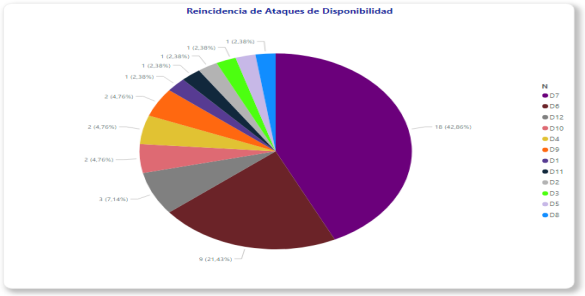


Fig. 6: Reincidencia Ataques de Disponibilidad.

Se detalla de manera específica estos ataques:

DDoS (D7): El ataque de denegación de servicios afecta principalmente a la disponibilidad de los datos que se encuentran en diferentes dispositivos. En [40] indica que debido a este ataque el sistema tienes fallos y niega el servicio a todo el personal autorizado, esto genera inconvenientes a los usuarios. En la figura 10 se visualiza que tiene un porcentaje de 42.86% de superioridad ante el resto de ataques.

Botnets (D6): Este ataque hace referencia a un grupo de dispositivos infectados con un malware malicioso, generando así una red de virus especiales que buscan una entrada en la seguridad de los dispositivos; una vez que se produzca esta red maliciosa se puede ejecutar varios ataques en grandes escalas. Como se observa en la figura 10 se tiene un porcentaje de 21.43%.

En la indagación de los ataques a la Integridad del estudio realizado se pudo constatar que existen varios ataques (ver tabla V), el que sobresale en esta investigación es Inyección de datos falsos (I5) con un porcentaje de 42.31% como se observa en figura 7

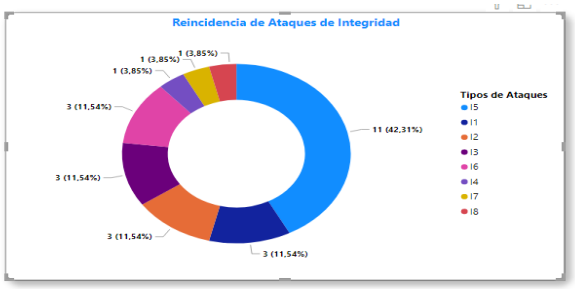


Fig. 7: Reincidencia Ataques de Integridad.

Inyección de datos falsos (I5): Ciberataque el cual se encuentra camuflado, el ciberdelincuente inserta un código malicioso de su autoría con la finalidad de vulnerar toda mediad de seguridad y así poder acceder a los datos, cuando el código se ejecuta adquiere el poder de tener un control total de la base de datos accediendo a datos personales.

En la indagación de los ataques a la Confidencialidad del estudio realizado se pudo constatar que existen varios ataques (ver tabla IV), los más relevantes son 2: Spoofing (C16), Pishing (C15) Y Scan (C9). (Ver figura 8)

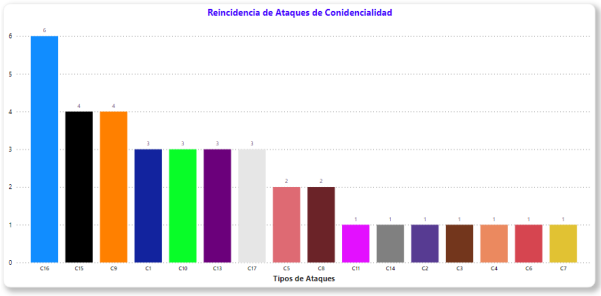


Fig. 8: Reincidencia Ataques de Confidencialidad.

Spoofing (C16): Conocido como suplantación de identidad, esto se refiere a que suplanta el origen de una fuente confiable, de esa manera accede a datos personales robando información, se puede dar a través de correos, mensajes, páginas web, etc. En el estudio tuvo un porcentaje de 16.22%.

Pishing (C15): Se basa en ingeniería social en la que imita correos electrónicos, páginas web y redes sociales, para entender de mejor manera este ataque el ciberdelincuente falsifica una red social similar a la red legítima, su método de propagación es a través de correo electrónico enviado enlaces falsos para obtener la información personal de la víctima. El ciberataque tuvo un porcentaje de en el estudio de 10.81%.

Scan (C9): Este ciberataque ataca directamente a los puertos de un dispositivo que se encuentre conectado a una red, ya que los analiza ca uno de estos y así lograr ingresar al equipo y

robar informaciones confidenciales de los usuarios. Tiene un porcentaje de estudio de 10.81%.

E. SLRP3 ¿Que ciberataques han recibido las capas en la infraestructura de ciudades inteligentes?

Existen elementos que se necesitan esencialmente para estar en una ciudad inteligente: edificios, servicios públicos e infraestructura, tecnologías modernas de información y comunicación, transporte y gestión del tráfico como se indica en [40] Estos componentes forman parte de las capas que integran la infraestructura de la ciudad inteligente (ver figura 2).

Cada una de las capas se han visto perjudicadas por ciberataques que pueden vulnerar los datos, afectando su confidencialidad, integridad y disponibilidad como se da a entender posteriormente en la tabla IX.

Capa	**Ataque**
Aplicación	I5,D7,D10,C4
Datos	C7,C1,D6
Comunicación	I7,D12,C7,I5
Detección	D6,C13,D7,C16,C15

Tabla IX: Ciberataques recibidos en las capas

F. SLRP4 ¿Cuál es el nivel de amenaza y taxonomía de usuarios en las ciudades inteligentes?

En la siguiente tabla ver (tabla X) se analiza el nivel de amenaza que tiene cada cliente cuando uno de sus dispositivos se ve afectado por un ciberataque o malware, en esta etapa describimos los cuatro niveles al que el cliente se encuentra expuesto al ser víctima de la delincuencia cibernética: Muy alto, Alto, Medio y Bajo.

Usuario	**Nivel de Amenaza**	**Descripción de Amenaza**
Persona Común	Bajo	Ciberataque que causará algún daño personal y que no tendrá mayor impacto en la sociedad y seguridad nacional.
Empresa	Medio	Ciberataque que puede causar pérdida de información a la propiedad corporativa donde se evidenciará pérdidas económicas, sin embargo, no tendrá ningún impacto en la sociedad y seguridad nacional.
Infraestructura	Alto	Ciberataque que afectará el funcionamiento de la sociedad y generará grandes pérdidas económicas y apenas perjudicará a la seguridad nacional.
Gobierno	Muy Alto	Ciberataque que provocará pérdidas significativas y efectos perjudiciales para la seguridad nacional.

Tabla X: Nivel de amenaza y taxonomía de usuarios

IV. Conclusiones

El SMap en el estado de arte contribuyó en la separación y reducción de las publicaciones más importantes de ciberataques en dispositivos de ciudades inteligentes. Para el desarrollo de SMap se implementaron tres ciclos donde se define los criterios de estudio por medio de la cadena de busqueda, se estableció preguntas de investigación y la exclusión de las publicaciones sustanciales las que inluyeron para los resultados de este estudio. El SLRev ayudó a visibilizar de mejor manera las investigaciones sobre los diferentes ciberataques a dispositivos de las ciudades inteligentes, entre los últimos 5 años de diferentes bases de datos.

En las publicaciones se han distinguido varios ataques que prejundican a ciertos dispositivos situados en las Smart cities, para determinar los ataques se llevo a cabo una una clasificación basada en la CIA . En los ataques que afectan a la confidencialidad los más habituales fueron C16, C15 y C9, donde el primer ataque destaca con un 16.22%, y los otros dos ataques restantes comparten el 10.81%.Los ataques que van contra la disponibilidad son D7 con un 42.86% y D6 con un 21.43 % . Por último, el ataque que afecta a la integridad es I5 con un 42.31% .

Como es de conocimiento cada acción tiene una reacción en el caso de los ataques cibernéticos no hay excepción, existen las técnicas de detección de ataques, estas se conforman por diversas áreas teniendo como objetivo desarrollar una solución inteligente, En las publicaciones estudiadas se han hallado varias técnicas con las cuales ha sido posible la detección de varios ciberataques que se han dado a los diferentes dispositivos que conforma las ciudades inteligentes, K-Nearest Neighbor (T12), Redes neuronales (T17) y Simulación (T20).

Con el auge de la tecnología los ciberdelincuentes se han dado las formas de realizar un ataque a los dispositivos que conforman las ciudades inteligentes, En la investigación realizada se ha descubierto 26 dispositivos que han sufrido algún tipo de ciberataque, de entre los cuales se han enfocado en 4, los cuales son: Redes, sensores, RFID y dispositivos móviles, estos dispositivos se han visto vulnerados por algún malware, que han sido detectados con técnicas de inteligencia artificial.

References

[1] R. O. Andrade, S. G. Yoo, L. Tello-Oquendo, and I. Ortiz-Garcés, "Cybersecurity, sustainability, and resilience capabilities of a smart city," in *Smart Cities and the un SDGs*. Elsevier, 2021, pp. 181–193.

[2] G. Maestre-Gongora and R. F. Colmenares-Quintero, "Systematic mapping study to identify trends in the application of smart technologies," in *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE, 2018, pp. 1–6.

[3] K. Ahmad, M. Maabreh, M. Ghaly, K. Khan, J. Qadir, and A. Al-Fuqaha, "Developing future human-centered smart cities: Critical analysis of smart city security, data management, and ethical challenges," *Computer Science Review*, vol. 43, p. 100452, 2022.

[4] A. Altaf, H. Abbas, F. Iqbal, M. M. Z. M. Khan, A. Rauf, and T. Kanwal, "Mitigating service-oriented attacks using context-based trust for smart cities in iot networks," *Journal of Systems Architecture*, vol. 115, p. 102028, 2021.

[5] K.-h. Son, B.-i. Kim, and T.-j. Lee, "Cyber-attack group analysis method based on association of cyber-attack information," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 14, no. 1, pp. 260–280, 2020.

[6] K. Ma. (2022, jun) Confidentiality, integrity and availability in cyber security. [Online]. Available: https://kobalt.io/confidentiality-integrity-and-availability-in-cyber-security/

[7] S. Ali and T. N. Malik, "Intrusion detection and prevention against cyber attacks for an energy management system," *Mehran University Research Journal Of Engineering & Technology*, vol. 41, no. 1, pp. 202–219, 2022.

[8] N. Koroniotis, N. Moustafa, and J. Slay, "A new intelligent satellite deep learning network forensic framework for smart satellite networks," *Computers and Electrical Engineering*, vol. 99, p. 107745, 2022.

[9] D. B. Rawat and K. Z. Ghafoor, *Smart cities cybersecurity and privacy*. Elsevier, 2018.

[10] A. AlDairi *et al.*, "Cyber security attacks on smart cities and associated mobile technologies," *Procedia Computer Science*, vol. 109, pp. 1086–1091, 2017.

[11] S. Gönen, H. H. Sayan, E. N. Yılmaz, F. Üstünsoy, and G. Karacayılmaz, "False data injection attacks and the insider threat in smart systems," *Computers & Security*, vol. 97, p. 101955, 2020.

[12] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and bot-iot attacks traffic identification for internet of things in smart city," *Future Generation Computer Systems*, vol. 107, pp. 433–442, 2020.

[13] X. Dai and L. Yao, "A classification method and implementation of trojan and botnet infected user based on threat matrix model," in *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*. IEEE, 2019, pp. 1231–1236.

[14] V. Kumar and D. Sinha, "A robust intelligent zero-day cyber-attack detection technique," *Complex & Intelligent Systems*, vol. 7, no. 5, pp. 2211–2234, 2021.

[15] Q. Chang, X. Ma, M. Chen, X. Gao, and M. Dehghani, "A deep learning based secured energy management framework within a smart island," *Sustainable Cities and Society*, vol. 70, p. 102938, 2021.

[16] B. Gupta, P. Chaudhary, X. Chang, and N. Nedjah, "Smart defense against distributed denial of service attack in iot networks using supervised learning classifiers," *Computers & Electrical Engineering*, vol. 98, p. 107726, 2022.

[17] J. Park, H. Chung, and J. F. DeFranco, "Multilayered diagnostics for smart cities," *Computer*, vol. 55, no. 2, pp. 14–22, 2022.

[18] S. Pazouki, K. Bibek, H. A. Alkhwaildi, and A. Asrari, "Modelling of smart homes affected by cyberattacks," in *2020 52nd North American Power Symposium (NAPS)*. IEEE, 2021, pp. 1–6.

[19] V. Prasanna Srinivasan, K. Balasubadra, K. Saravanan, V. Arjun, and S. Malarkodi, "Multi label deep learning classification approach for false data injection attacks in smart grid," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 15, no. 6, pp. 2168–2187, 2021.

[20] M. A. Lawal, R. A. Shaikh, and S. R. Hassan, "A ddos attack mitigation framework for iot networks using fog computing," *Procedia Computer Science*, vol. 182, pp. 13–20, 2021.

[21] W. Serrano, "The blockchain random neural network for cybersecure iot and 5g infrastructure in smart cities," *Journal of Network and Computer Applications*, vol. 175, p. 102909, 2021.

[22] H. Alsulami, "Implementation analysis of reliable unmanned aerial vehicles models for security against cyber-crimes: Attacks, tracebacks, forensics and solutions," *Computers and Electrical Engineering*, vol. 100, p. 107870, 2022.

[23] S. N. Narayanan, K. Khanna, B. K. Panigrahi, and A. Joshi, "Security in smart cyber-physical systems: a case study on smart grids and smart cars," in *Smart cities cybersecurity and privacy*. Elsevier, 2019, pp. 147–163.

[24] I. K. Preet and K. S. Saini, "A systematic evaluation of literature on internet of things (iot) and smart technologies with multiple dimensions," *Journal of Technology Management for Growing Economies*, vol. 11, no. 1, pp. 1–10, 2020.

[25] K. K. Nguyen, D. T. Hoang, D. Niyato, P. Wang, D. Nguyen, and E. Dutkiewicz, "Cyberattack detection in mobile cloud computing: A deep learning approach," in *2018 IEEE wireless communications and networking conference (WCNC)*. IEEE, 2018, pp. 1–6.

[26] A. A. Jahromi, A. Kemmeugne, D. Kundur, and A. Haddadi, "Cyber-physical attacks targeting communication-assisted protection schemes," *IEEE Transactions on Power Systems*, vol. 35, no. 1, pp. 440–450, 2019.

[27] M. Mohammadpourfard, A. Khalili, I. Genc, and C. Konstantinou, "Cyber-resilient smart cities: Detection of malicious attacks in smart grids," *Sustainable Cities and Society*, vol. 75, p. 103116, 2021.

[28] I. Lee, "Internet of things (iot) cybersecurity: Literature review and iot cyber risk management," *Future Internet*, vol. 12, no. 9, p. 157, 2020.

[29] F. Moazeni and J. Khazaei, "Formulating false data injection cyberattacks on pumps' flow rate resulting in cascading failures in smart water systems," *Sustainable Cities and Society*, vol. 75, p. 103370, 2021.

[30] W. Wang, G. Cova, and E. Zio, "A clustering-based framework for searching vulnerabilities in the operation dynamics of cyber-physical energy systems," *Reliability Engineering & System Safety*, vol. 222, p. 108400, 2022.

[31] S. Chakrabarty and D. W. Engels, "Secure smart cities framework using iot and ai," in *2020 IEEE Global Conference on Artificial Intelligence and Internet of Things (GCAIoT)*. IEEE, 2020, pp. 1–6.

[32] P. K. Chouhan, L. Chen, T. Hussain, and A. Beard, "A situation calculus based approach to cognitive modelling for responding to iot cyberattacks," in *2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI)*. IEEE, 2021, pp. 219–225.

[33] T. Gaber, A. El-Ghamry, and A. E. Hassanien, "Injection attack detection using machine learning for smart iot applications," *Physical Communication*, vol. 52, p. 101685, 2022.

[34] O. Ajayi and T. Saadawi, "Detecting insider attacks in blockchain networks," in *2021 International Symposium on Networks, Computers and Communications (ISNCC)*. IEEE, 2021, pp. 1–7.

[35] N. Z. Bawany and J. A. Shamsi, "Seal: Sdn based secure and agile framework for protecting smart city applications from ddos attacks," *Journal of Network and Computer Applications*, vol. 145, p. 102381, 2019.

[36] M. Snehi and A. Bhandari, "Vulnerability retrospection of security solutions for software-defined cyber–physical system against ddos and iot-ddos attacks," *Computer Science Review*, vol. 40, p. 100371, 2021.

[37] S. Bhowmick, B. Halo, and S. Panja, "Bipartite consensus control of multi-agent systems under multiple denial-of-service cyber attacks," *IFAC-PapersOnLine*, vol. 55, no. 1, pp. 697–702, 2022.

[38] B. Bordel, R. Alcarria, T. Robles, and Á. Sánchez-Picot, "Stochastic and information theory techniques to reduce large datasets and detect cyberattacks in ambient intelligence environments," *IEEE Access*, vol. 6, pp. 34 896–34 910, 2018.

[39] A. K. Sangaiah, A. Javadpour, F. Ja'fari, P. Pinto, H. Ahmadi, and W. Zhang, "Cl-mlsp: The design of a detection mechanism for sinkhole attacks in smart cities," *Microprocessors and Microsystems*, vol. 90, p. 104504, 2022.

[40] J. Al-Muhtadi, K. Saleem, S. Al-Rabiaah, M. Imran, A. Gawanmeh, and J. J. Rodrigues, "A lightweight cyber security framework with context-awareness for pervasive computing environments," *Sustainable Cities and Society*, vol. 66, p. 102610, 2021.

[41] G. Falco, A. Viswanathan, C. Caldera, and H. Shrobe, "A master attack methodology for an ai-based automated attack planner for smart cities," *IEEE Access*, vol. 6, pp. 48 360–48 373, 2018.

[42] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer networks*, vol. 169, p. 107094, 2020.

[43] C. Ma, "Smart city and cyber-security; technologies used, leading challenges and future recommendations," *Energy Reports*, vol. 7, pp. 7999–8012, 2021.

[44] S. Praharaj, "Area-based urban renewal approach for smart cities development in india: Challenges of inclusion and sustainability," *Urban Planning*, vol. 6, no. 4, pp. 202–215, 2021.

[45] M. M. Salim, S. K. Singh, and J. H. Park, "Securing smart cities using lstm algorithm and lightweight containers against botnet attacks," *Applied Soft Computing*, vol. 113, p. 107859, 2021.

[46] S. Sengan, V. Subramaniyaswamy, S. K. Nair, V. Indragandhi, J. Manikandan, and L. Ravi, "Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart

network," *Future generation computer systems*, vol. 112, pp. 724–737, 2020.
[47]
[48] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for iot-based smart grid networks," *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 36–49, 2019.
[49] R. O. Andrade, S. G. Yoo, L. Tello-Oquendo, and I. Ortiz-Garcés, "Cybersecurity, sustainability, and resilience capabilities of a smart city," in *Smart Cities and the un SDGs*. Elsevier, 2021, pp. 181–193.
[50] A. R. S. A. Cruz, R. L. Gomes, and M. P. Fernandez, "An intelligent mechanism to detect cyberattacks of mirai botnet in iot networks," in *2021 17th International Conference on Distributed Computing in Sensor Systems (DCOSS)*. IEEE, 2021, pp. 236–243.
[51] J. Ashraf, M. Keshk, N. Moustafa, M. Abdel-Basset, H. Khurshid, A. D. Bakhshi, and R. R. Mostafa, "Iotbot-ids: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities," *Sustainable Cities and Society*, vol. 72, p. 103041, 2021.
[52] M. Azimian, V. Amir, S. Javadi, S. Mohseni, and A. C. Brent, "Resilience-oriented planning of multi-carrier microgrids under cyber-attacks," *Sustainable Cities and Society*, vol. 79, p. 103709, 2022.
[53] H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata, "A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities," *Sustainable Cities and Society*, vol. 50, p. 101660, 2019.
[54] S. Yan, S. K. Nguang, and L. Zhang, "Nonfragile integral-based event-triggered control of uncertain cyber-physical systems under cyber-attacks," *Complexity*, vol. 2019, 2019.
[55] Z. E. Huma, S. Latif, J. Ahmad, Z. Idrees, A. Ibrar, Z. Zou, F. Alqahtani, and F. Baothman, "A hybrid deep random neural network for cyberattack detection in the industrial internet of things," *IEEE Access*, vol. 9, pp. 55 595–55 605, 2021.
[56] N. N. Sapavath, E. Muhati, and D. B. Rawat, "Prediction and detection of cyberattacks using ai model in virtualized wireless networks," in *2021 8th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2021 7th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. IEEE, 2021, pp. 97–102.
[57] K. N. Qureshi, S. S. Rana, A. Ahmed, and G. Jeon, "A novel and secure attacks detection framework for smart cities industrial internet of things," *Sustainable Cities and Society*, vol. 61, p. 102343, 2020.
[58] S. Rani, A. Kataria, M. Chauhan, P. Rattan, R. Kumar, and A. K. Sivaraman, "Security and privacy challenges in the deployment of cyber-physical systems in smart city applications: State-of-art work," *Materials Today: Proceedings*, 2022.
[59] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. A. Kazmi, and C. S. Hong, "Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges," *Future Generation Computer Systems*, vol. 92, pp. 265–275, 2019.
[60] K. U. Nisa, A. Alhudhaif, K. N. Qureshi, H. J. Hadi, and G. Jeon, "Security provision for protecting intelligent sensors and zero touch devices by using blockchain method for the smart cities," *Microprocessors and Microsystems*, vol. 90, p. 104503, 2022.
[61] L. Hou, Y. Li, W. Luo, and H. Sun, "Adaptive tracking control of switched cyber-physical systems with cyberattacks," *Applied Mathematics and Computation*, vol. 415, p. 126721, 2022.
[62] Y. Yılmaz and S. Uludag, "Timely detection and mitigation of iot-based cyberattacks in the smart grid," *Journal of the Franklin Institute*, vol. 358, no. 1, pp. 172–192, 2021.
[63] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for iomt networks," *Computer Communications*, vol. 166, pp. 110–124, 2021.
[64] S. Sengan, V. Subramaniyaswamy, V. Indragandhi, P. Velayutham, and L. Ravi, "Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning," *Computers & Electrical Engineering*, vol. 93, p. 107211, 2021.
[65] A. Joby. What is k-nearest neighbor? an ml algorithm to classify data. [Online]. Available: https://learn.g2.com/k-nearest-neighbor
[66] I. d. l. Nava Ortego, "Aprendizaje profundo en la extracción de información de documentos de identidad," Ph.D. dissertation, ETSI_Informatica, 2020.
[67] S.N. Network devices explained. [Online]. Available: https://blog.netwrix.com/2019/01/08/network-devices-explained/
[68] D. V.-B. S. Y. D. R. G. S. S. Hamdi Kavak, Jose J Padilla, "Simulación para ciberseguridad: estado del arte y direcciones futuras," in *Journal of Cybersecurity*, ser. 1, vol. 7, 2021.