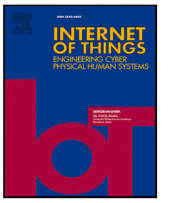
Internet of Things 22 (2023) 100792

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot



Review article

Anomaly-based cyberattacks detection for smart homes: A systematic literature review

Juan Ignacio Iturbe Araya [a,b,*], Helena Rifà-Pous [a,c]

[a] Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya (UOC), Barcelona, Spain
[b] Departamento de Ingeniería Informática, Universidad de Santiago de Chile, Santiago, Chile
[c] Center for Cybersecurity Research of Catalonia (CYBERCAT), Barcelona, Spain

ARTICLE INFO

Keywords:
Anomaly detection
Machine Learning
Internet of Things (IoT)
Smart home
Cybersecurity
Cyber attacks
Systematic literature review (SLR)

ABSTRACT

Smart homes, leveraging IoT technology to interconnect various devices and appliances to the internet, enable remote monitoring, automation, and control. However, collecting sensitive personal and business data assets renders smart homes a target for cyberattacks. Anomaly detection is a promising approach for identifying malicious behavior in smart homes. Yet, the current literature primarily discusses IoT-related cyberattacks and gives limited attention to detecting anomalies specific to the smart home context. Furthermore, there is a lack of datasets that accurately represent the complexity inherent in a smart home environment in terms of users with varying levels of expertise and diverse, evolving types of devices. Therefore, this paper presents a systematic literature review (SLR) that focuses on using anomaly detection to identify cyberattacks in smart home environments. The SLR includes an adapted taxonomy that classifies existing anomaly detection methods and a critical analysis of the current state of knowledge and future research challenges. Our findings show a growing interest in detecting cyberattacks with anomaly-based models in smart homes using centralized and network-based features. Ensemble and deep learning techniques are popular methods for detecting these anomalies. However, the limited diversity of cyberattacks in existing datasets and the absence of comprehensive datasets representing the complexity of smart home environments call for further research to improve the generalizability of detection models.

1. Introduction

Digital assets protection from cyberattacks is a significant concern as society is becoming digital. These assets can include operational data, Personally Identifiable Information (PII), or strategic information; and are generated, stored, and transferred in organizations, homes, and personal devices. Particularly, the protection of homes has taken relevance with the rise of telecommuting, and smart homes must receive special attention.

Smart homes are an attractive target for cybercriminals due to the lack of user technical knowledge, insecure Internet of Things (IoT) devices, inadequate configurations, poor implementation of controls, and the high value of the digital assets involved. The IoT industry has grown exponentially; it is expected to grow to 48 billion connected devices by 2023 [1]. However, new vulnerabilities have been continuously discovered and threats have emerged. Indeed, everyday new cyberattacks (zero-day attacks) exploit these weaknesses with enormous potential damage.

* Corresponding author at: Departamento de Ingeniería Informática, Universidad de Santiago de Chile, Santiago, Chile.
E-mail address: jiturbea@uoc.edu (J.I.I. Araya).

https://doi.org/10.1016/j.iot.2023.100792
Received 26 January 2023; Received in revised form 23 March 2023; Accepted 14 April 2023
Available online 28 April 2023

Anomaly-based Detection Systems (ADS) are a promising approach to detect unknown cyberattacks. ADS is a complex field that attempts to distinguish between abnormal and normal behavior. These systems work by establishing a baseline of normal behavior and they continuously monitor the network or device to flag suspicious deviations. Due to the changing behavior of users and cyberattackers, the most difficult aspect of this field is keeping the models up-to-date [2].

ADS demonstrates promising results in IoT security [3], but implementing these solutions in the context of smart homes is a significant challenge. Because these environments involve many user-device interactions. Moreover, the heterogeneity of these environments makes it difficult to create ADS that can be implemented in any smart home. Indeed, user behavior can change over time, and new occupants can move into a home. In addition, the devices, model brands, communication systems, protocols, and digital assets in each residence can vary considerably. A smart home environment has very high risks. Therefore, it is necessary to have defense systems that can adapt to the environment and detect both old and new cyberattacks without requiring a model update. The principal contributions of this SLR are listed as follows:

- A comprehensive discussion about the potential cybersecurity threats of smart homes.
- In-depth review of the ADS for smart homes.
- A taxonomy to classify anomaly detection methods.
- A review of issues, challenges, gaps, and future directions.

The remainder of this article has the following composition. Section 2 provides a background of smart home features and architectures, anomaly detection systems, metric evaluations, and presents an anomaly detection taxonomy. Section 3 shows the SLR process. Section 4 analyzes the obtained results and answers the research questions. Section 5 discusses the latter results, and some research proposals for the future are made. Finally, Section 6 concludes the work.

2. Background

In this article, a systematic literature review (SLR) is developed, which requires a review of several concepts and taxonomies for the selection and categorization of articles. Concepts of what a smart home is and the many types of cyberattacks that can affect these environments can be found in the literature and will be covered in further detail below. However, no taxonomies on anomaly detection approaches used by researchers in the field have been identified. Therefore, we have developed a taxonomy based on what already exists to classify the selected papers.

2.1. Smart homes

There are several definitions of smart home in the literature. One of the first definitions found in the literature is found in [4]. The authors define smart home as "a home that incorporates a communications network that connects major appliances and electrical services and allows them to be remotely controlled, monitored, or accessed" (p. 659). In addition, there are eleven additional definitions in [5].

The concepts outlined in the previous definitions suggest that by integrating intelligent devices and tailored services, a dwelling can enhance its potential, efficiency, and comfort. A connected home typically includes communication hardware, motion sensors, and smart appliances such as refrigerators, lights, washing machines, televisions, heating, ventilation, and air conditioning (HVAC) systems. These components work together to enable the home to provide amenities such as entertainment, warmth, and illumination through centralized management of automated appliances.

Additionally, these smart tools are capable of autonomously fulfilling a wide array of demands, including retrieving information, tracking food inventory, activating washing machines, supplying entertainment, and regulating ambient temperature. By incorporating these technologies and services, a smart home can greatly improve the quality of life for its inhabitants, providing a more convenient, enjoyable, and easy daily living experience.

An automated home is not synonymous with a smart home. A computerized house performs actions based on previously programmed activities. In contrast, a home is smart when all the data about its environment is stored and analyzed, patterns are detected, and automated decisions are made based on these [6]. Smart homes can collect and analyze data on their inhabitants and surroundings to acquire and apply this knowledge in their environment.

2.2. Threats taxonomies

In the literature, there are several taxonomies for the classification of threats. Some are general taxonomies [7,8], and others are focused on specific fields. Among those that focus on IoT [9–11], there is no consensus on the categories to use. Cyber threat taxonomies for smart homes are an emerging field of study [12], and they are insufficiently complete and usable.

In this study, we have chosen to employ the STRIDE threats taxonomy [13]. The STRIDE taxonomy has been implemented because it is widely used for modeling cyber–physical system threats [14–24]. STRIDE is a taxonomy developed by Microsoft where each letter of its name alludes to a general threat. The meaning of each, the cybersecurity property affected and its definition are specified in Table 1. All possible smart home cyberattacks have been classified according to the STRIDE scheme, as detailed in the following sections.

Table 1
STRIDE taxonomy.

Threat	Property	Definition	Example
Spoofing	Authentication	Pose as something or somebody else, such as legitimate users, processes, or system elements.	An attacker spoofing the MAC address of a smart device to gain access to a network.
Tampering	Integrity	Modification or edition of legitimate data or code.	An attacker who manipulates the firmware of a smart home device to gain unauthorized access to the device or the network.
Repudiation	Non-Repudiation	Denying to have performed a particular action than other parties can neither ratify nor refuse.	A homeowner denying having issued certain commands to the home automation system, despite evidence suggesting otherwise.
Information Disclosure	Confidentiality	Data breach or unauthorized access to confidential information.	An attacker intercepting and reading sensitive information such as user credentials, network traffic or sensor data from a smart home system, leading to potential privacy violations and unauthorized access.
Denial of Service	Availability	Interruption of service to legitimate users.	An attacker overwhelming a smart device with traffic so it cannot function properly.
Elevation of Privilege	Authorization	Obtaining higher privileged access to system elements by a restricted user.	An attacker gains elevated access to a smart home device by exploiting a vulnerability in its firmware, allowing them to perform actions beyond their intended level of access.

2.3. Cyberattacks

Each smart home's environment is unique, making it susceptible to a wide range of threats and cyberattacks. Cyberattacks are logical threats that manifest via computer networks and devices. They have evolved or taken on new forms since the beginning of computer networks and the Internet (e.g., denial of service, sniffing, and probing, among others). Some of them are unique on IoT, the ones related to the characteristics of emerging IoT devices (low processing capacity, topologies, and device development focused solely on their functionality). A smart home contains IoT devices, so the cyberattacks above may be utilized against a smart home if appropriate vulnerabilities exist. There are a number of cyberattacks currently in existence. Several of these have existed since the beginning of communication networks and can be applied to any network type, including IoT. Typically, these types of attacks target network infrastructures with interconnected heterogeneous devices and active user interaction. Subsequently, we present our categorization of various cyberattacks in Table 2, based on the STRIDE model, its definitions, and main characteristics derived from a thorough analysis of pertinent studies in the field, following the methodological approach outlined in Section 3.

- Denial of Service (DoS): the attacker uses the device's resources to affect its service availability. For instance, an attacker consumes a device's processing power and network bandwidth, resulting in the device becoming unresponsive and affecting its service availability. Smart home devices are especially susceptible to this type of attack due to their low processing capabilities and can even be affected by low rate DoS [25].
- Flooding (FLD): the attacker sends massive quantities of requests or data to a legitimate service, server, or network to deny their normal use. For instance, an attacker flooding a smart home device or network with many requests, packets or messages, potentially causing it to become overwhelmed and unable to respond to legitimate traffic, affecting its availability and performance [26].
- Probing (Prob): Probing is a technique used by attackers to scan networks or devices with the intent of gathering information about their structure, vulnerabilities, and weaknesses. This information can then be exploited to launch other types of cyberattacks or steal sensitive data. In a smart home context, a probing cyberattack may involve an attacker using tools such as Nmap [27], a widely-used network scanning utility, to examine a smart home device's network. By identifying open ports and available services, the attacker can gain insights into potential vulnerabilities in the system. Once these weaknesses are discovered, the attacker can then target the identified open ports with further attacks, such as a Distributed Denial of Service (DDoS) attack [26] which can severely impact the functionality and security of the smart home system.

Table 2
Classification of cyberattacks in smart home based on the STRIDE taxonomy.

Cyberattack	S	T	R	I	D	E
Denial of Service (DoS)					✓	
Flooding (FLD)					✓	
Probing (Prob)				✓		
Distributed DoS (DDoS)					✓	
Botnet (BN)	✓					
Man in The Middle (MiTM)	✓					
Brute Force (BF)						✓
Injection		✓				
Spoofing (SP)	✓					
Replay attack (RP)		✓				
Jamming attack					✓	
User-to-root (U2R)						✓
Remote-to-Local (R2L)						✓
Deauth attack					✓	
Sink hole attack				✓		
Keylogging attack				✓		
Masquerade (MSQ)	✓					
Delay attack					✓	
Ransomware					✓	

- Distributed Denial of Service (DDoS): the attacker coordinates multiple malicious nodes to launch a focused cyberattack on a target [28]. In these attacks, a large network of compromised devices, such as Internet of Things (IoT) and smart homes devices, are used to flood a targeted server with requests [29]. This attack overwhelms the server, rendering it unresponsive and affecting the availability of its services. One of the most devastating examples of a DDoS attack was the attack on DNS provider Dyn, which originated from a botnet called Mirai that consisted of compromised IoT devices and smart homes. This attack had far-reaching consequences, causing disruptions for numerous major websites, including Amazon, Airbnb, GitHub, Netflix, PayPal, Reddit, The New York Times, and Visa [30].
- Botnet (BN): the attacker managed several devices by exploiting vulnerabilities. For instance, an attacker uses malware to infect multiple smart devices and then uses them to carry out coordinated attacks, such as DDoS attacks or data theft, which can significantly impact the security and functionality of the smart home network and devices. One of the biggest attacks on the Internet was the one caused by the Mirai botnet in 2016, which infected more than 600k devices, such as IP cameras, DVRs, VoIP phones, routers, and printers, causing a large number of DDoS attacks, highlighting the potential dangers of botnets [31].
- MiTM: the attacker intercepts communication between two parties, often altering the content of the communication without either party knowing [26]. For instance, an attacker gains access to a smart home network and intercepts communication between a smart thermostat and the home automation system, altering temperature settings without the owner's knowledge. Altering temperature settings through a man-in-the-middle attack can be dangerous because it can lead to significant discomfort or damage to the home. This was the case of a family that saw their nest security system compromised, repeatedly setting it too high temperatures [32].
- Brute Force (BF): the attacker guesses passwords until the right one is found. For instance, an attacker attempting to gain access to a device or network by repeatedly trying different password combinations until the correct one is found, potentially allowing them to take control of the device or access sensitive information, compromising the security and privacy of the users and the overall system.
- Injection: The attacker tries to modify the packets or data to include malicious content in the nodes. For instance, an attacker alters network packets to change the content of a message or injects malicious code, potentially causing a smart home device to malfunction, leak sensitive information, or compromise the security of the whole system [26].
- Spoofing (SP): the attacker hides their identity by, for example, sending packets with a fake IP source. For instance, an attacker impersonates a legitimate device or user by faking a MAC or IP address, allowing them to bypass authentication and access the network, steal data or launch other types of cyberattacks [26].
- Replay attack (RP): the attacker intercepts network communications and delays or re-sends them to mislead the recipient. For instance, an attacker intercepts and records network traffic containing authentication or command messages and replays them later to gain unauthorized access to the network or control over a smart home device, compromising its security and privacy [28].
- Worm: This malicious software, upon implanted in a device, aims to self-replicate and transmit to other devices via the network [33]. The attacker controlling the worm can then inflict substantial harm on the intended target. Hypothetically, it has been suggested that a worm might propagate by leaping from an infected light source to adjacent ones using their ZigBee connectivity. Due to the absence of verification among Philips Hue bulbs, the attack can continue to expand unhindered [34].
- Fuzzer: A tool for enhancing software reliability, which employs a multitude of arbitrary inputs to identify system weaknesses or failures [35]. Attackers might use this approach to discover zero-day vulnerabilities for malicious purposes. Study [36] introduces a framework for detecting potential security issues in Z-Wave IoT smart home devices via fuzz testing.

- Backdoor: this is a method used to bypass the authentication and encryption barriers of a device and create secret access that allows access and control without the user's knowledge [37]. In Study [38], IoT backdoors like Crypto (using flawed algorithms), Systems (avoiding authentication), and Hardware (utilizing physical flaws) are discussed, emphasizing potential hazards and intrusion methods.
- Exploit: A piece of software that takes advantage of a vulnerability, often with malicious intent, such as installing malware [39]. In study [40], the authors identify common vulnerabilities in smart home devices that are frequently targeted for exploit development, including outdated protocols, weak encryption, constrained storage and processing capabilities, insecure applications, inadequate authentication, firmware flaws, and heterogeneous architecture.
- Jamming attack: the attacker seeks to block the wireless communications medium from a source node to a receptor node. For instance, an attacker transmits a high-powered signal on the same frequency as a ZigBee video surveillance camera, disrupting its communication ability and affecting its functionality [26].
- User-to-root (U2R): the attacker exploits device vulnerabilities for root access. For instance, an attacker exploits a vulnerability in a smart home device's firmware or software to gain elevated privileges and take control of the device (such as cameras, routers, printers), potentially accessing other devices and data in the network and compromising the security and privacy of the whole system. This category of attacks comes from the KDD99 dataset [41].
- Remote-to-Local (R2L): the attacker gets unauthorized access to resources in a network. For instance, an attacker exploits a vulnerability in a smart home device's cloud service to gain access to the user's local network, allowing them to control other devices in the network, such as smart locks or cameras, and potentially cause physical harm to the occupants. This category of attacks also comes from the KDD99 dataset [41].
- Deauth attack: an attacker sends de-authentication frames to a wireless access point, which can force a device to disconnect from a Wi-Fi network. For instance, an attacker could employ a laptop and a deauth attack tool to send de-authentication frames to a smart home security camera, causing the camera to lose its connection to the Wi-Fi network. This could expose the home to intruders and other security concerns [42].
- Sinkhole attack: the attacker redirects traffic from its intended destination to a server under his control, allowing him to intercept and manipulate it. For instance, an attacker gains unauthorized access to a smart home network and creates a dummy device that impersonates the functionality of a security camera, routing traffic to a server under the attacker's control. This could enable an attacker to intercept and manipulate communications on the smart home network, granting them access to sensitive information or the ability to control connected devices [26].
- Keylogging attack: the attacker records keystrokes made by the user, allowing them to capture sensitive information like login credentials or financial information. For instance, An attacker gains unauthorized access to a smart home network and installs keylogging software on a connected device, like a computer or tablet, to capture keystrokes made by the user. This can allow the attacker to gain access to sensitive information, like login credentials or financial information, which can be used to gain access to other accounts or devices connected to the smart home network, ultimately endangering the security and privacy of the home [43].
- Impersonation or Masquerade attack: the attacker gains unauthorized access using a fake identity. For instance, an attacker impersonates a legitimate user or device by using stolen or spoofed credentials, allowing them to gain unauthorized access to the smart home network and control devices or steal sensitive information, compromising the security and privacy of the users and the overall system. This type of case is common when smart home users do not change the default credentials of their IoT devices, so access to them is much easier [25].
- Delay attack: the attacker delays normal network communication. For instance, an attacker intentionally delays the delivery of network packets to a smart home device, causing it to become unresponsive or fail to perform an action in a timely manner, potentially affecting its overall functionality and usability. This attack is especially easy to implement since it does not depend on vulnerabilities in smart home devices nor on key/token leaks [44].
- Ransomware: the attacker is able to install malicious software that encrypts files or systems, often requiring payment in exchange for access to the data or system. In a smart home environment, an attacker may gain unauthorized access to a smart home network and use ransomware to encrypt files on devices, like security cameras or thermostats, depriving the owner of access to vital information and control over their smart devices, ultimately endangering the security and privacy of their home [45].

2.4. Intrusion Detection Systems

The IDS are a mechanism to detect cyberattacks. These systems can adopt different configurations, architectures, and strategies in order to detect cyberattacks. IDS can be classified according to their detection strategies, placement strategies, and validation strategies. Also, some evaluation metrics are necessary to prove systems performance, accuracy, and implementation feasibility.

2.4.1. Detection strategy

The way how an IDS tries to detect a cyberattack varies in function of the strategy adopted. The ones widely used in the literature are described below.

- Signature-based IDS: Also named rule-based or misuse IDS. This IDS has a database that saves patterns and signatures of well-known attacks. If an observed behavior matches one of these rules, detection is done. This type of IDS needs to be continuously updated [46].

- Anomaly-based IDS: It uses models, statistics or rules in order to predict abnormal behavior. The models or rules are based on heuristics techniques or artificial intelligence methods. These methods classify the activity between normal or abnormal according to a threshold. A more comprehensive explanation can be found in Section 2.5.
- Specification-based IDS: It is similar to the ADS approach. However, this is based on specifications manually developed and captures legitimate system behaviors. It detects irregular behavior outside the defined rules. These specifications can be created based on security policies [46]. an IDS with this strategy can monitor inside the node operation in an IoT environment to assure that nodes follow all the routing rules [47].
- Hybrid IDS: It combines signature-based, anomaly-based, and specification-based intrusion detection systems (IDS) for enhanced performance. This approach produces fewer false positives and false negatives than previous methods, but it requires more processing power to execute signature-based and ADS modules in parallel.

2.4.2. Placement strategy

There are three main strategies for implementing an Intrusion Detection System (IDS), which are centralized, distributed, and hybrid. The definitions of these strategies are as follows:

- Centralized: IDS is implemented in a single node. The IDS decision is based on their observations.
- Distributed (DIDS): The detection system is located in the different devices across the network. Each device collects and analyzes the data from its environment and detects the intrusion.
- Hybrid: This case combines centralized and distributed architectures to obtain the best qualities. For instance, an IDS centralized analyze the incoming traffic from the Internet and detect external attacks, and on distributed nodes, IDS detects internal attacks.

2.4.3. Validation strategy

IDS validation strategies are helpful to conclude when an IDS model is a close enough representation of the system detecting attacks. To validate the effectiveness of IDS, authors have used techniques such as theoretical, empirical, and hypothetical strategies [48]. There are many metrics to evaluate an IDS. However, each of these metrics must be used according to their specific context. Some essential factors must consider designing an IDS, such as low false alarm rate, use of resources, and the ability to detect real-time threats. For these proposes, metrics are used to evaluate them, such as:

- Accuracy: a metric that calculates the overall rate of detection and false alarms an IDS model produces.
- Detection Rate (DR), also called True Positive Rate (TPR), Hit Rate, Sensitivity or Recall: the proportion of malicious instances correctly classified.
- Precision (Prec.): measures the ratio of malicious instances was correct.
- False Positive Rate (FPR), also called False Alarm Rate: the normal behavior rate classified as a cyberattack.
- False Negative Rate (FNR): the cyberattack instance rate classified as normal.
- True Negative Rate (TNR), also called specificity: the chance that an actual normal class will test normal.
- F1-Score or F-measure: a measure of accuracy calculated from precision and recall. It is helpful when the class labels are unbalanced or skewed. This metric calculates the harmonic mean of precision and recall and provides a single weighted metric to assess the overall classification performance.

2.5. Anomaly detection

Anomalies are data instances that do not match the expected behavior. According to [49], anomalies or outliers are “substantial variations from the norm”. Anomalies can appear in the data for several reasons, such as malicious activity or fault, for instance, credit card fraud, hackers intrusions, and system malfunctions. All these problems are critical to detect by an analyst [50]. There are three types of anomalies [51]:

- Point Anomaly: occurs when only one instance of data is considered an anomaly from the rest of the data.
- Contextual Anomalies: occurs when data is abnormal in a specific context but not in another context.
- Collective Anomalies: occurs when an associated data instance is abnormal for a data set.

Anomaly detection can be categorized into three categories according to the availability of labeled data. The three categories are [50]:

- Supervised anomaly detection: we have a set of data labeled normal and anomaly. From these data a model is built to predict that a new instance is normal or an anomaly.
- Semi-supervised anomaly detection: only instances of normal classes are included for model generation. New samples that cannot be classified as normal are an anomaly.
- Unsupervised anomaly detection: no training labeled data is needed to build the classification model.

Several taxonomies are appreciated in the literature for anomaly detection methods [50,52–55]. However, these taxonomies are inconsistent in their categorization of methods (not considering soft computing methods or the combination of models for classifier generation). As a result, from the previous taxonomies, we consolidate, propose, and use the following general taxonomy with the following categories:

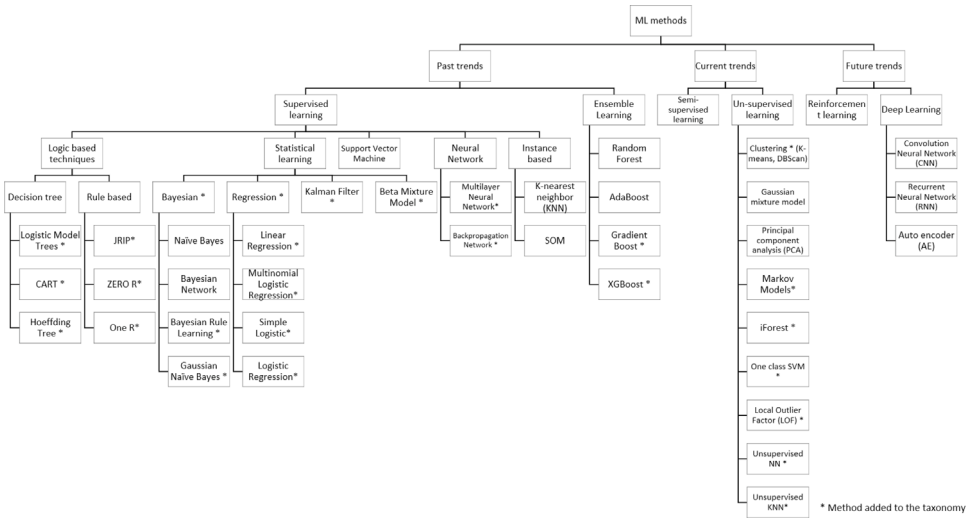


Fig. 1. Machine learning methods taxonomy. Based on Gupta et al. [56].

- Classification-based [50,53,54]: methods that create a model (classifier) from a collection of labeled data instances (training) and then classifying a test instance using the learned model (test).
- Combination Learners [53]: it is used through weighted combinations of several methods, typically classifiers.
- Clustering-based [50,53,54]: methods that group objects into clusters such that they are more similar than those in other clusters.
- Information Theory [50,54]: methods that analyze a data set's information using information-theoretic measurements like complexity, entropy, and relative entropy.
- Nearest Neighbor-based [50]: methods that presume typical data examples occur in dense neighborhoods and abnormalities far from their nearest neighbors.
- Soft computing-based [53]: methods for which there are frequently no exact solutions such as genetic algorithms, artificial neural networks, fuzzy sets, rough sets, ant colony algorithms and artificial immune systems.
- Spectral [50]: methods that map high-dimensional data to a lower-dimensional representation.
- Statistical-based [50,52,53,55]: methods based on the assumption that normal data instances occur in high-probability regions of a stochastic model and anomalies occur in low-probability regions of the stochastic model.

Most articles selected for Section 3 identify anomalies using machine learning techniques. Therefore, it was decided to include a second taxonomy to examine these methods from a different angle. Gupta et al. [56] propose a taxonomy to organize machine learning models used in secure data analytics. First, they include supervised learning machine learning classic methods, and ensemble learning in past trends. Second, current trends include semi-supervised and unsupervised learning. Finally, future trends include deep learning (DL) and reinforcement learning. However, this categorization does not include all the methods in the SLR below. Therefore, the taxonomy was complemented with these methods (marked with an asterisk) in Fig. 1.

3. The review process

This article provides state of art on ADS in smart home environments. Systematic Literature Review (SLR) is used to provide "a means of evaluating and interpreting all available research relevant to a particular research question or topic area or phenomenon of interest" [57]. The advantages of SLR from a conventional expert literature review are:

- It is less likely that their results are biased.
- It can provide synthesized information about the effects of some phenomenon across a wide range of settings and empirical methods.
- In the case of quantitative studies, it is possible to combine data using meta-analytic techniques.

The phases of SLR are planning, conducting, and reporting (see Fig. 2).

3.1. Planning phase

3.1.1. Identify the need for a review

To establish the necessity for a systematic revision, the first step entails looking for and analyzing relevant literature reviews on ADS for smart homes. This research was conducted using review articles from 2015 to 2022. Accordingly, as far as we are aware,

Fig. 2. Systematic literature review phases.

there is no survey focusing on ADS for smart homes. Table 3 lists research works that are most closely related to our current study by the number of citations (one full star corresponds to approximately 100 citations). IoT ADS dominates the majority of these literature reviews. Additionally, none of them consider the complexities of a smart home environment.

3.1.2. Research questions

This SLR intends to examine, identify, and summarize research about the detection of cyberattacks using anomalies in smart home contexts from 2015 through 2021 inclusive. We formulated six research questions (RQs) for this purpose:

- RQ1: How much research on anomaly detection of cyberattacks for smart homes has there been since 2015?
- RQ2: What are the strategies to detect, place and validate an ADS for smart homes?
- RQ3: What are the best ADS methods to detect cyberattacks on smart homes context?
- RQ4: Which are the metrics used to evaluate an ADS in a smart home context?
- RQ5: Which are the source datasets and features to train and test the models?
- RQ6: What are the research gaps and future challenges Anomaly Detection of Cyberattacks for smart homes?

3.1.3. Review protocol

We define a review protocol based on the SLR methodology to reduce the risk of researcher bias. The protocol defines the article collection and selection, quality assessment checklists, data extraction, and synthesis strategies. By using a clear protocol and strict rules for what to include and what to leave out, the review is more objective and transparent, which makes the results more valid and reliable. The review is also a chance to judge the quality of the literature and find any flaws or biases in the research. The following sections show the main procedures of our review protocol and how this is applied.

3.2. Conducting phase

3.2.1. Article collection

In this activity, we created a search strategy to retrieve all the relevant studies that answer the research questions. We collected articles using the search terms in Table 4 for the selected data sources and years. This search was conducted in February 2023, so

Table 3
Related reviews (see [58–85]).

Art.	Year	ADS	Smart home	IoT	Attacks	ML	DL	Other methods	SLR	Citations
[58]	2017	◑	○	●	●	○	○	●	○	★★★★★★★
[59]	2018	●	○	●	●	●	●	●	○	★★★★★
[60]	2020	●	○	●	●	●	●	●	○	★★★½
[61]	2018	○	●	●	●	○	○	○	○	★★★
[46]	2018	●	◑	●	◑	●	●	●	○	★★½
[62]	2020	◑	○	●	●	○	●	●	○	★★
[63]	2019	●	○	●	●	○	○	●	○	★½
[43]	2015	○	●	○	●	○	○	○	○	★½
[64]	2019	●	○	●	●	◑	○	○	○	★
[65]	2018	●	○	●	●	○	○	●	○	★
[48]	2021	●	○	●	●	●	●	●	○	★
[66]	2020	◑	◑	●	●	●	●	○	○	★
[67]	2021	●	○	●	◑	●	●	●	●	★
[68]	2020	●	○	●	○	●	●	○	○	★
[69]	2021	◑	○	●	●	●	●	●	●	★
[70]	2019	●	○	●	●	●	○	●	○	½
[71]	2019	◑	○	●	◑	●	●	○	○	½
[72]	2021	●	○	●	●	●	○	●	○	½
[73]	2020	◑	○	●	●	◑	●	○	●	½
[74]	2021	●	○	●	●	●	●	○	○	½
[75]	2021	●	◑	●	○	●	●	○	○	½
[76]	2022	○	●	○	●	○	○	○	○	½
[77]	2020	●	○	●	◑	●	○	○	○	½
[78]	2022	○	●	●	●	○	○	○	○	½
[79]	2021	◑	○	●	◑	●	●	○	○	½
[80]	2021	●	○	●	◑	●	○	○	○	
[81]	2022	○	●	○	○	○	●	○	●	
[82]	2021	◑	○	●	●	◑	◑	○	○	
[83]	2022	◑	○	◑	◑	●	●	○	○	
[3]	2022	●	○	●	◑	○	○	○	○	
[84]	2022	○	●	●	●	○	○	○	○	
[85]	2022	◑	○	●	○	◑	●	○	○	
This SLR	2022	●	●	●	●	●	●	●	●	

the digital library indexers may not yet have added research from the latter part of 2022. The search strategy has the following two-step procedure:

- Define search criteria based on relevant keywords: We adopt the steps proposed by Brereton et al. [86] to build the search query shown in Table 4:
  - Decompose the research questions into individual terms.
  - Collect keywords from known primary articles for other main terms.
  - Identify synonyms for the main terms.
  - Define search strings using Boolean "AND" to connect main terms and "OR" to incorporate synonyms.
- Determine the source for the relevant studies: The list of sources focused on the online digital libraries, journals, and conference proceedings relevant to this research interest. We select the following digital libraries to be searched:
  - Web of Science.
  - Scopus.
  - IEEE Xplore.
  - ACM Digital Library

3.2.2. Article selection

The selection and filtration steps included in this SLR are defined below:

i. Eliminate non-journal and non-conference papers.

Table 4
Search query.

(anomal* OR detect* OR IDS) AND (attack*) AND (“smart home” OR smarthome* OR “home computing” OR “home automation” OR “smart building” OR “smart buildings” OR “smart house” OR “connected home” OR domotics)

ii. Remove the duplicated articles that are found in different libraries.
iii. Apply inclusion and exclusion criteria.

- Inclusion criteria:
  - Include the newest edition of the article if different versions are available.
  - Include quantitative research.
  - Include the articles published between 2015 to 2022.
  - All articles must be published in the English language.
- Exclusion criteria:
  - Exclusion by title, abstract, and keywords.
  - All the articles that do not complain about the inclusion criteria.
  - Exclude papers unrelated to ADS of cyberattacks in a smart home environment.
  - Exclude qualitative research.

iv. The methodology emphasizes the importance of assessing the quality of the articles. Adapted questions from the methodology and a set of rules for evaluating the quality of the articles served this purpose [87]. The Quality Assessment Rules (QAR) consist of a series of questions to which the possible answers are Y=1 (Yes), P=0.5 (Partially), *N* (Not), or Unknown=0. Each QAR equals one (1) out of ten points (10). The article was considered if the sum of all QAR was at least six; otherwise, it was discarded.

- QA1: Are the research questions or objectives clearly defined?
- QA2: Is the study put into the context of other studies and research?
- QA3: Are the detection or prediction methods used clearly defined?
- QA4: Are the proposed methods and their results compared with other techniques?
- QA5: Are the methods setting parameters specified?
- QA6: Are the datasets used publicly available?
- QA7: Is the source of anomaly data described (specific cyberattacks, malfunction, among others)?
- QA8: Are the features used clearly defined? (packet parameters, logs, network traffic statistics, among others)?
- QA9: Are the evaluation metrics well described and justified?
- QA10: Are all study questions or objectives answered evidence-based?

v. Search for additional related articles from the article references obtained from step iv. and repeat from i. on the extra article.

Fig. 3 shows an overview of the results of Conducting phase. Applying the previously defined review protocol reduced the number of papers from 1438 to 98. Table 5 lists the selected articles.

3.2.3. Data extraction

For each selected paper, the following data has been extracted:

- Method with best result and compared methods: support vector machine (SVM), decision tree (J48), naive bayes (NB), random forest (RF), k-nearest neighbors (k-NN), hidden markov model (HMM), principal components analysis (PCA), ensemble strategy (ES), or own method.
- Detection strategy: ADS, signature-based, hybrid.
- Placement strategy: centralized or distributed.
- Validation strategy: hypothetical, simulation, or empirical.
- Source of features: network traffic, user behavior, or sensor data.
- Used dataset: dataset name or own creation.
- Dataset availability: public, on request, or not available (NA).
- Dataset source: laboratory, simulation software, or smart home Environment.
- Anomaly data source: specifics cyberattacks, several cyberattacks, malicious device, faulty device, anomalies as a potential cyberattack.
- Evaluation metrics: ROC, accuracy (Acc.), true positive Rate (TPR), false positive rate (FPR), true detection rate (TDR), false detection rate (FDR), detection ratio (DR), miss-detection ratio (MR), processing time (time), specificity (SP), recall, f-score (F-S), precision (Prec.), or other.

Table 5
Selected articles.

Num.	Ref	Year	Author	Num.	Ref	Year	Author
1	[88]	2016	Nobakht et al.	50	[89]	2020	Al Mtawa et al.
2	[90]	2016	Al Baalbaki et al.	51	[91]	2020	Liu et al.
3	[92]	2017	Kanev et al.	52	[93]	2020	Pacheco et al.
4	[94]	2017	Bhunia et al.	53	[95]	2020	Tertytchny et al.
5	[96]	2017	Midi et al.	54	[97]	2020	Galeano-Brajones et al.
6	[98]	2018	Pacheco et al.	55	[99]	2021	Azumah et al.
7	[100]	2018	Brun et al.	56	[101]	2021	Atul et al.
8	[102]	2018	Roux et al.	57	[103]	2021	Sikder et al.
9	[104]	2018	McDermott et al.	58	[105]	2021	Alsabilah et al.
10	[106]	2018	Bhatt et al.	59	[107]	2021	Cvitic et al.
11	[108]	2018	Liu et al.	60	[109]	2021	Krishna et al.
12	[110]	2018	Doshi et al.	61	[111]	2021	Elsayed et al.
13	[112]	2018	Meidan et al.	62	[113]	2021	Alkahtani et al.
14	[114]	2019	Mohammed et al.	63	[115]	2021	Khurma et al.
15	[116]	2019	Anthi et al.	64	[117]	2021	Ashraf et al.
16	[118]	2019	Shahid et al.	65	[119]	2021	Heartfield et al.
17	[120]	2019	Pacheco et al.	66	[121]	2021	Bobrovnikova et al.
18	[122]	2019	Yamauchi et al.	67	[123]	2021	Shi et al.
19	[124]	2019	Ramapatruni et al.	68	[125]	2021	Qaddoura et al.
20	[126]	2019	Paudel et al.	69	[127]	2021	Ullah et al.
21	[128]	2019	Nguyen et al.	70	[129]	2021	Aljumah, A.
22	[130]	2019	Procopiou et al.	71	[131]	2021	Kumar et al.
23	[132]	2019	Subbarayalu et al.	72	[133]	2021	Tawfik et al.
24	[134]	2019	Sharma et al.	73	[135]	2021	Yamauchi et al.
25	[136]	2019	Zhou et al.	74	[137]	2021	Krishnan et al.
26	[138]	2019	Wang et al.	75	[139]	2021	Amraoui et al.
27	[140]	2019	Dilraj et al.	76	[141]	2021	Nakagawa et al.
28	[142]	2019	Gajewski et al.	77	[143]	2022	Jia et al.
29	[144]	2019	Salman et al.	78	[145]	2022	He et al.
30	[146]	2019	Khraisat et al.	79	[147]	2022	Gazdar, T.
31	[148]	2019	Hasan et al.	80	[149]	2022	Yadav et al.
32	[150]	2019	Tang et al.	81	[151]	2022	Diallo, C.
33	[152]	2020	Alghayadh et al.	82	[153]	2022	Oshio et al.
34	[154]	2020	Spanos et al.	83	[155]	2022	Das et al.
35	[156]	2020	Yamauchi et al.	84	[157]	2022	Sohail et al.
36	[158]	2020	Maniriho et al.	85	[159]	2022	Baz, M.
37	[160]	2020	Mafarja et al.	86	[161]	2022	Almaraz-Rivera et al.
38	[162]	2020	Zhang et al.	87	[163]	2022	Tariq et al.
39	[164]	2020	Khare et al.	88	[165]	2022	Nimmy et al.
40	[166]	2020	Alghayadh et al.	89	[167]	2022	Meidan et al.
41	[168]	2020	Hegde et al.	90	[169]	2022	Dai et al.
42	[170]	2020	Yuan et al.	91	[171]	2022	Ramana et al.
43	[172]	2020	Wan et al.	92	[173]	2022	Shukla et al.
44	[174]	2020	Sahu et al.	93	[175]	2022	Li et al.
45	[176]	2020	Li et al.	94	[177]	2022	Butt et al.
46	[178]	2020	Toutsop et al.	95	[179]	2022	Dat-Thinh et al.
47	[180]	2020	Gassais et al.	96	[181]	2022	Anand et al.
48	[182]	2020	Eskandari et al.	97	[183]	2022	Alonazi et al.
49	[184]	2020	Alghayadh et al.	98	[185]	2022	Gupta et al.

3.2.4. Data synthesis

The data must be synthesized to answer each research question. Activities related to data synthesis can be found in Section 4.

4. Results

This section explains and discusses the results of our SLR while answering the established research questions.

4.1. RQ1: How much research on Anomaly Detection of Cyberattacks for smart homes has there been since 2015?

The volume of research on the anomaly detection of cyberattacks in smart home contexts has increased in the last few years. Fig. 4 summarizes related works according to their publication year from 2015 to 2022. However, a significant number of research articles were published during 2019–2022, indicating a growing interest in the field. Indeed, in 2019, a drastic increment of 100% in research activity can be seen. Later, the research activity was stabilized in the years 2020, 2021, and 2022. This interest could be related to necessary telecommuting due to the COVID-19 pandemic. In addition, Fig. 5 shows the published paper's distribution according to its source and database. The figure suggests that the majority of the research is done in conferences. It also indicates that most discussions occur in the IEEE Xplore Database.

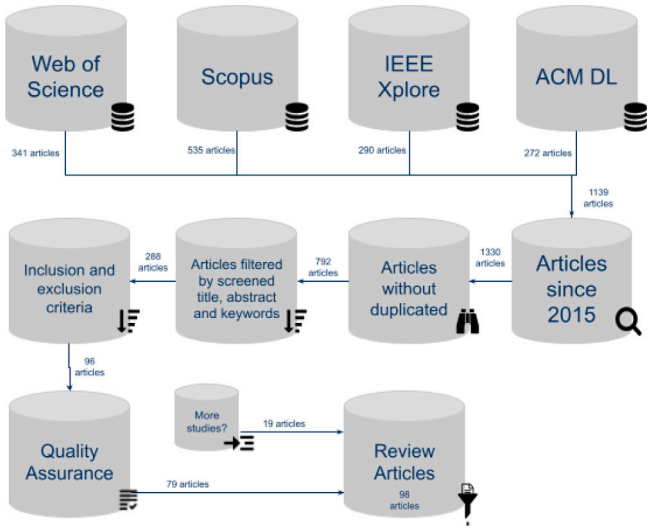


Fig. 3. SLR conducting phase results.

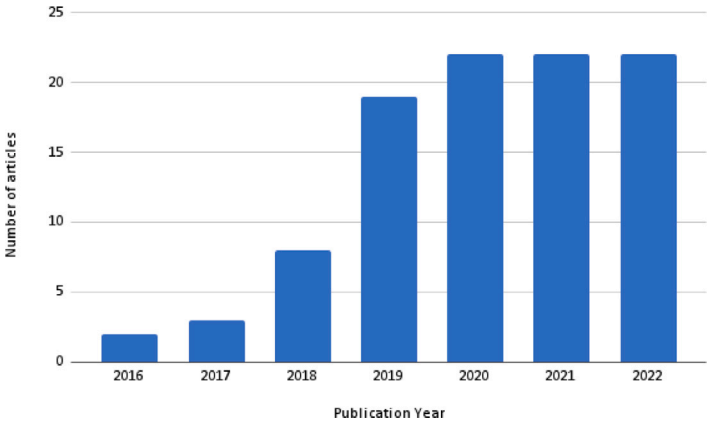


Fig. 4. Publication by year.

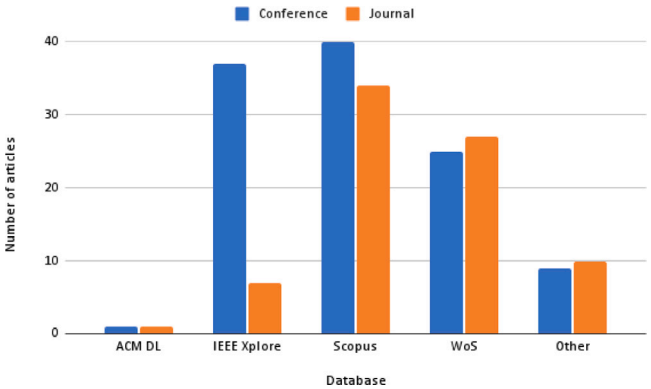


Fig. 5. Published papers distribution.

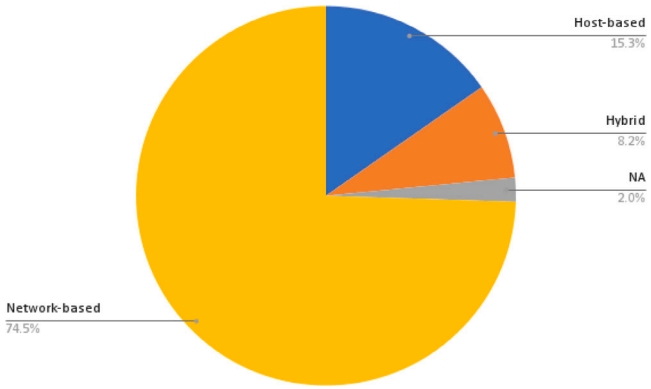


Fig. 6. IDS type.

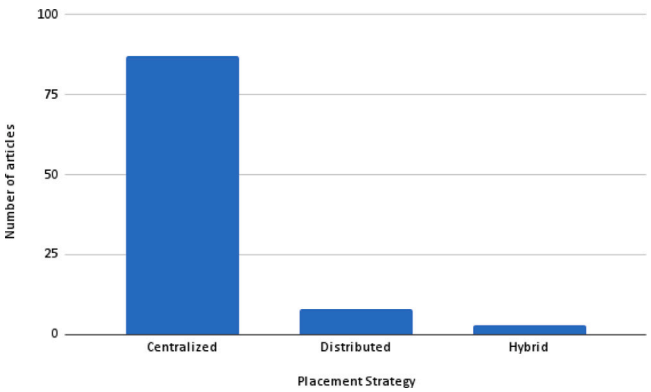


Fig. 7. Placement strategy.

4.2. RQ2: What are the strategies to detect, place, and validate an ADS for smart homes?

Network-based detection, centralized placement, and empirical validation are the most common strategies to detect cyberattacks on smart homes contexts. On the one hand, most public datasets use networks as a source of data, and the researchers evaluate their models in an empirical and centralized way. On the other hand, datasets built by researchers mainly capture traffic from smart home networks in one strategic place. They then process and extract features to generate a unique dataset. Fig. 6 shows the distribution of detection strategies in the reviewed literature. Nearly 74.5% of reviewed papers use network-based detection, 15.3% use host-based detection [88,93,105,120,140,148,150,180,186] and 8.2% use hybrid detection schemes [119,121,123,124,152,166]. Fig. 7 shows that the most commonly used approach by researchers is centralized (nearly 90%), the distributed approach accounts for 8.2% [136,186,187], and 3.1% use a hybrid approach [96,150]. Based on the above, the distributed strategy is not very advisable in a single home due to the low processing capacity. However, it could be suitable if it is implemented in several homes. For example, the authors of propose, [123,145] propose two- and three-layer architectures. In particular, [187] proposes that the Internet Service Provider (ISP) be in charge of coordinating this architecture.

Fig. 8 illustrates the various detection approaches employed by researchers for detecting cyberattacks. Most researchers aim to detect two [88,95–97,101,104,110,114,119,126,130,138,140,150,154] or multiple cyberattacks [90,92,94,98,99,102,103,106,108,109,111,115–117,123,125,127–129,132,144,146,148,152,158,160,162,164,168,170,172,174,176,180,182,184,188] using their classifiers. Conversely, numerous researchers concentrate on detecting a single type of attack, such as DDoS, which has been particularly problematic in the IoT context [89,93,100,105,107,112,118,120–122,124,156,178]. Additionally, some researchers operate under the assumption that anomalies are indicative of cyberattacks. Lastly, a smaller group of researchers focuses on detecting malicious devices to prevent further infection or potential attacks, as well as identifying malfunctioning devices.

4.3. RQ3: What are the best ADS methods to detect cyberattacks on smart homes context?

Ensemble learning is the best-performing and most widely used method or strategy (see Fig. 9). Among the ensemble learning methods, random forest [91,109,110,114,144,148,152,158,162,178,184] stands out among all others. On the other hand, DL is another set of methods that stands out. The most widely used algorithms in this category are the convolutional neural network

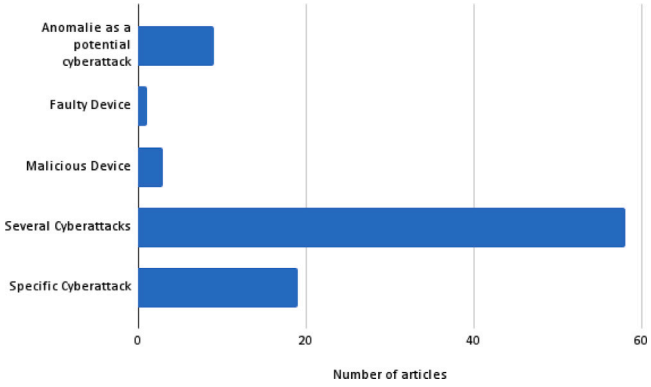


Fig. 8. Detection focus.

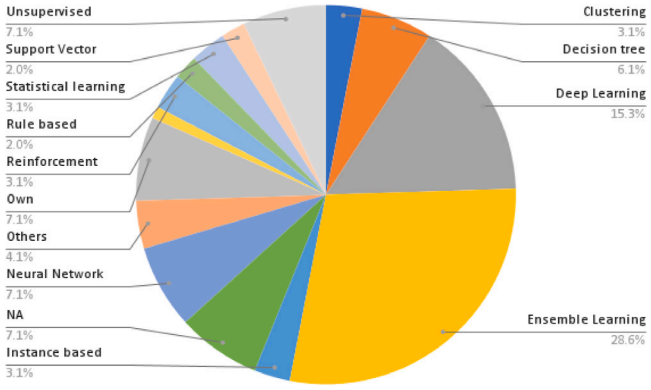


Fig. 9. Best results methods overall according to ML Taxonomy.

(CNN) [108,111,127,170] and the autoencoder [102,112,118]. Finally, other categories that stand out are the supervised machine learning methods decision tree (DT) [89,101,116,168,176,178], neural networks (ANN) [92,93,120,168,174], and instance-based, with the k-nearest neighbors method [89,115,160,172,184] standing out in this last category. Fig. 10 shows the evolution of using these methods over the last few years to obtain the best results. Ensemble learning and DL methods have dominated the best results in the last four years. Moreover, the last few years have seen a wide variety of techniques to improve detection results. Most of the results obtained in the review are very good in terms of their evaluation metrics. However, when implementing these systems in a real environment, it must be considered that they must be retrained with data from the particular environment. Additionally, labeling a dataset specifically for a particular household is not feasible for the supervised and semi-supervised methods. Therefore, strategies must be sought to implement these systems through methods that adapt to the environment and its changes. For example, through reinforcement learning [119,163] or transfer of learning [189].

An anomaly detection taxonomy is presented in Section 2.5. According to this taxonomy, it can be seen that the combination-based strategy outperforms all other categories (refer to Figs. 11 and 12). In fact, over a quarter of articles have used these techniques to achieve their best results. Another category that stands out is the one that contains the methods based on soft computing. The next most commonly used methods include classification-based, self-created, nearest neighbor-based, and clustering methods. However, in most cases, combination learners use classifier-based methods as part of themselves so that the result can be misleading.

4.4. RQ4: Which are the metrics used to evaluate an ADS in a smart home context?

Fig. 13 shows the evaluation metrics most commonly used in the articles of this review. The most used metric is precision, found in most reviewed articles. In addition, other metrics that stand out above the rest are accuracy, recall, f-score, and detection rate. All these metrics are typically used in the evaluation of machine learning classifiers. Likewise, they all depend on the fundamental metrics, i.e., true positives, false positives, true negatives, and false negatives.

Other important metrics are time and resource usage. These metrics are used because resources are limited in the smart home context. On the time side, they measure sorting times, training times [114,116,128,129,150], processing times [96,120,134,154,180,182], and latency [180], among others. On the other hand, researchers measure RAM [96,120,134,180,182,186], CPU [96,120,134,154,180,182], and bandwidth usage [134,182] on the resource usage side.

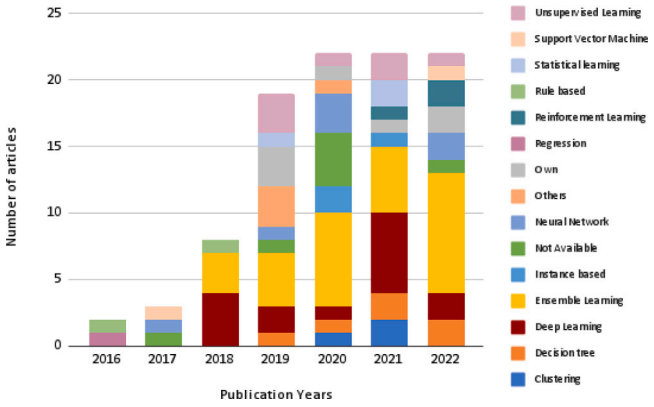


Fig. 10. Best results methods over the years according to Machine Learning Taxonomy.

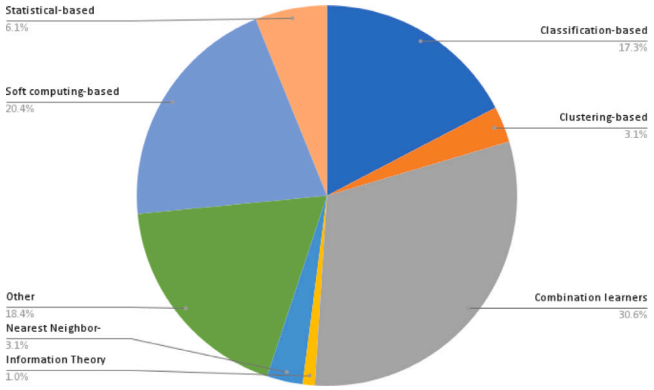


Fig. 11. Best results methods overall according to Anomaly Detection Taxonomy.

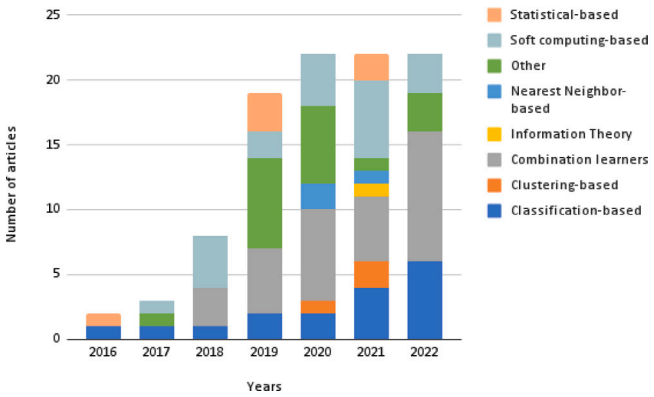


Fig. 12. Best results methods over the years according to Anomaly Detection Taxonomy.

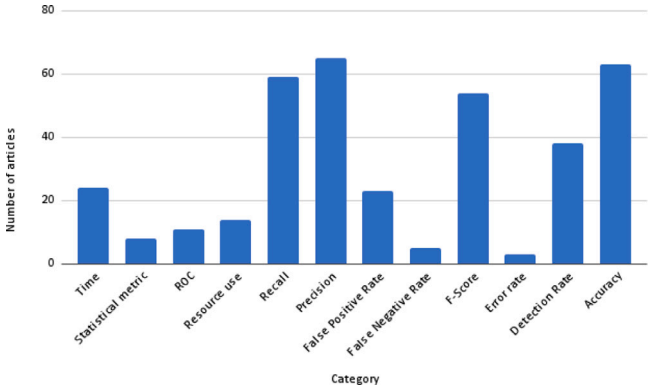


Fig. 13. Most used evaluation metrics.

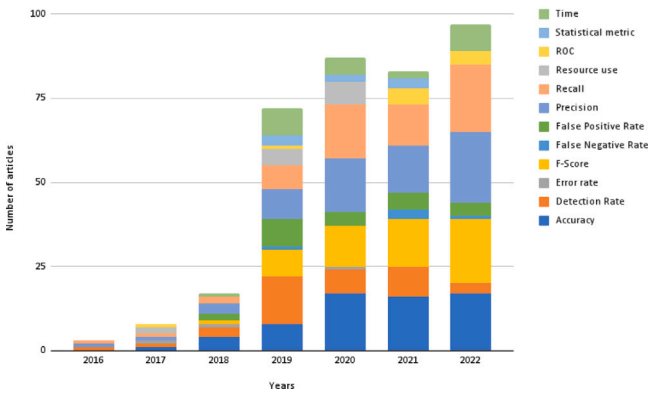


Fig. 14. Evaluation metrics evolution.

In recent years, the use of several evaluation metrics has evolved. The metrics that have been maintained over time include precision, accuracy, and recall. We assume this is because they are typical classification model evaluation criteria. In contrast, time measures and the f-score have gained prominence during the past four years. This is related to the fact that the characteristics of the IoT or smart home environment are increasingly being considered. On the one hand, resources are limited, so training and detection times must be fast; on the other hand, normal data is common, and cyber-attacks are rather infrequent (unbalanced data sets); thus, context-aware metrics provide more information. Fig. 14 depicts the evolution of the metrics over the years.

4.5. RQ5: Which are the source datasets and features to train and test the models?

Fig. 15 displays the distribution of datasets used by researchers in the reviewed articles. The analysis reveals that nearly half of the researchers used self-generated datasets to conduct their experiments, while the remaining used publicly available datasets [88–90,92–96,98,100–107,110,114,116,118–122,124,128,130,132,136,138,140,142,144,154,156,162,172,176,180,182,186]. However, the self-generated datasets researchers most do not report whether the datasets are accessible to other researchers (Fig. 16). In contrast, a wide variety of public datasets are used in these studies. For example, some of the most commonly used public datasets include IoT Botnet [48,97,123,127,129,162], IoT Network [91,99,111,117,127,178], and N-BaIoT [112,115,160]. In addition, a set of datasets are not representative of a smart environment but are still used by researchers: CSE-CIC-IDS2018 [144,152,184], UNSW-NB15 [170], NSL-KDD [109,184], and KDD99 [108]. For example, CSE-CIC-IDS2018 is a dataset that contains traffic from a local area network with servers, desktops, and other devices typical of a local area network. Other datasets are probably less used because they have been developed recently, for example, IoT-23 (2020) [127,168] and IoTID20 (2020) [113,125,158]. These findings emphasize the importance of problem-specific datasets in research while also highlighting the need for sharing such datasets to improve the reproducibility and generalizability of results. It is crucial to recognize that automated homes are not synonymous with smart homes, and datasets for studying these systems should account for the diverse interactions between individuals and devices to facilitate informed decision-making and a comfortable living experience.

Only eight of the fifteen public data sets used in the articles in this review contain data related to smart home environments. In Table 6, it is possible to see, over the years, what kind of data each public dataset contains and how it is utilized. Some articles focus on anomaly detection in smart home environments but use datasets that do not necessarily contain smart home data. In contrast,

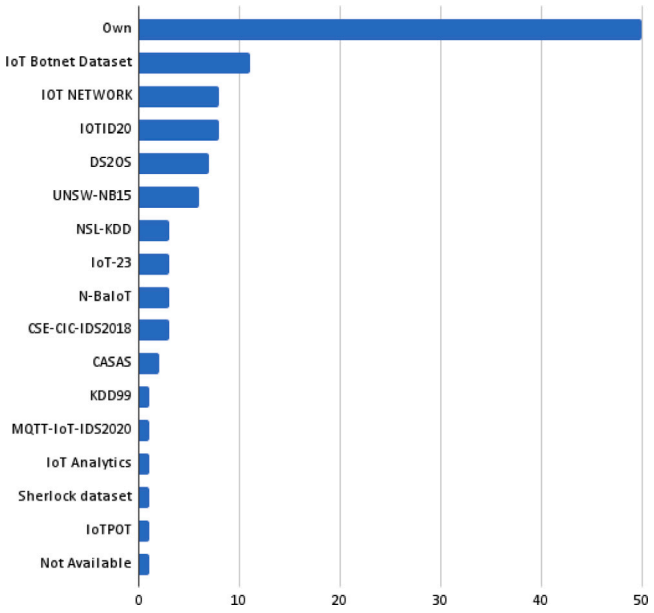


Fig. 15. Datasets distribution.

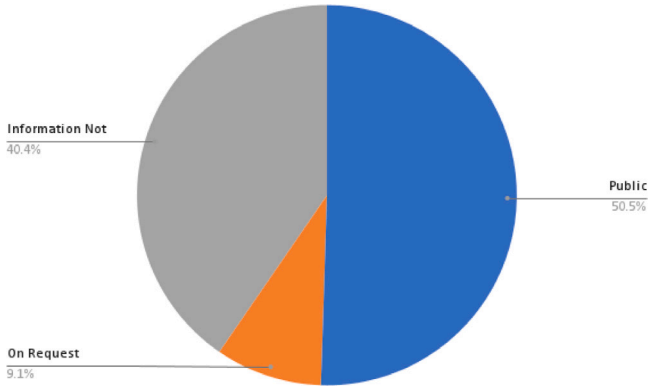


Fig. 16. Datasets availability.

since 2018, approximately 90% of datasets have been generated using smart homes as a data source. In addition, 75% of the articles that utilize public datasets also utilize datasets containing smart home data. To ensure the effectiveness of cyberattack detection systems in real-world smart home environments, it is crucial for researchers to use datasets with diverse inhabitants and devices, as this will help maintain security metrics when these systems are deployed.

The datasets used in smart home research, as shown in Fig. 17, can be classified into three categories based on their origin: laboratory, real smart home environment, and software simulation. Most of the papers generate smart home environments in their laboratories and simulate the behavior of smart devices. Also, 36% of the papers develop their datasets with real smart home environments [91,96,99,102,103,111,113,117–119,124–127,150,158,172,176,178,180,182]. Finally, the minority of the papers generate their datasets with software simulations [92,94,95,101,105,110,130,132,136,140,142,150,162]. To improve the adoption of ADS in real environments and decrease the problem of the high false positive rate, it is important that the training and evaluation data come from real smart home environments.

The researchers of the selected articles rely heavily on network traffic-derived characteristics. As shown in Fig. 18, network traffic-derived characteristics are commonly used in smart home research due to their ease of acquisition and applicability across different smart home and IoT environments. In particular, network and transport protocol header parameters and traffic statistics are used as features. For detecting DoS cyberattacks, for instance, the latter was primarily used. On the other hand, researchers use fewer features from sensor data or hosts. We think user behavior features (those features that model user behavior) are the least used because they are hard to get and model. The use of network characteristics for the detection of attacks in smart home environments is appreciated since the network traffic will be found in any smart home network. However, not all cyber attacks occur on the

Table 6
Datasets used by articles.

Ref	Year	Dataset name	Smart home	Generic IoT	LAN	Other	Used by
[41]	1999	KDD99	–	–	✓	–	[108]
[190]	2009	NSL-KDD	–	–	✓	–	[109,155,184]
[191]	2009	CASAS	✓	–	–	–	[139,150]
[192]	2015	UNSW-NB15	–	–	✓	–	[151,155,170, 171,173,177]
[193]	2015	IoTPOT	–	✓	–	–	[118]
[194]	2016	Sherlock dataset	–	–	–	✓	[134]
[112]	2018	N-BaIoT	✓	✓	–	–	[112,115,160]
[195]	2018	CSE-CIC-IDS	–	–	✓	–	[144,152,155, 171,179,184]
[196]	2018	DS2OS	✓	–	–	–	[139,143,148, 149,155,164, 174]
[197]	2019	Bot-IoT	✓	✓	✓	–	[97,123,127,129, 137,146,159, 161,162,171, 173,179]
[198]	2019	IoT Network Intrusion	✓	–	–	–	[91,99,111,117, 127,131,151, 178]
[199]	2019	IoT Analytics	✓	✓	–	–	[126]
[200]	2020	IoTID20	✓	–	–	–	[113,125,133, 157–159,179, 183]
[201]	2020	IoT-23	✓	–	–	–	[127,145,168]
[202]	2020	MQTT-IoT-IDS	–	✓	–	–	[127]
[203]	2020	TON-IoT	–	✓	✓	✓	[147,159,162, 181]

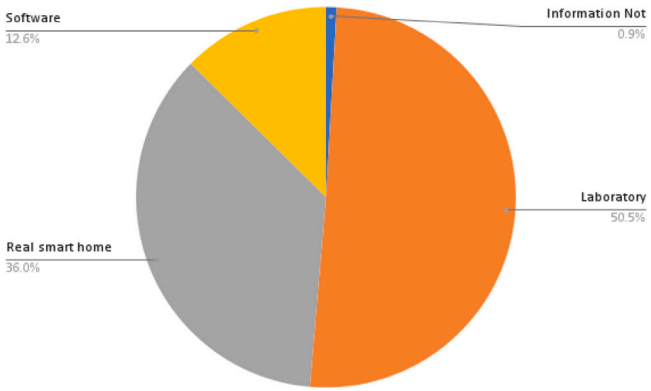


Fig. 17. Datasets origin.

network but can be executed on hosts, on devices, or are directed at communication devices or the physical transmission medium, so there remains uncertainty as to whether these systems are capable of detecting these other types of attacks.

Fig. 19 depicts the threats identified by STRIDE. The most frequently discussed attacks in the articles include denial of service, information leakage, and spoofing. For instance, scanning, Man-in-the-Middle (MitM), botnet, DoS, and DDoS attacks appear most frequently in datasets. Scanning is one of the first steps in a cyberattack because it helps hackers find possible targets. It is essential to spot this attack because it helps with a proactive plan to protect the smart home. For example, if this attack is identified, its source can be found, and the attack can be stopped. Another common attack is MiTM attack, which is important to detect in smart homes because it helps find a malicious device that may be altering or leaking information from the smart home. Additionally, the detection of malicious devices within a botnet-controlled network is investigated. Some of the worst attacks in recent years have come from IoT devices in smart homes that were taken over by botnets and used in DoS or DDoS attacks. The research has focused on DoS and scanning cyberattacks (classified as information disclosure in STRIDE), then to a lesser extent, those of the spoofing and tampering type; however, there are cyberattacks that do not fall into these categories. These would be taken into account during the investigations, especially those related to the elevation of privileges and repudiation. According to us, this restriction is inherent

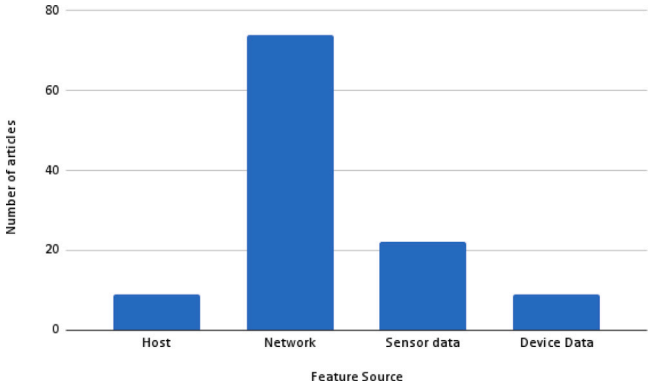


Fig. 18. Datasets features.

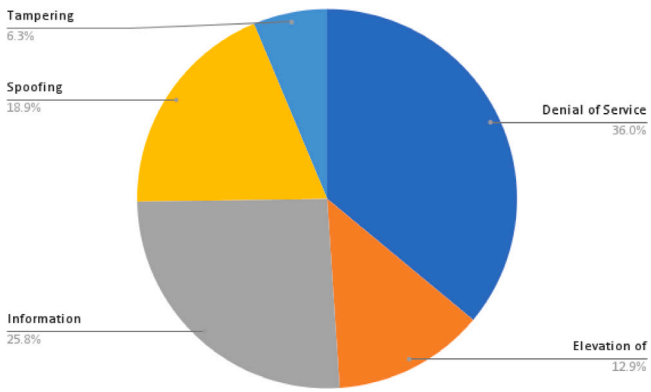


Fig. 19. STRIDE threats in research articles.

to the origin of the data, as network-based attacks are carried out on the hosts themselves. Thus, building hybrid systems that can detect host and network threats becomes essential.

Table 7 lists the cyberattacks described in the selected articles. The most common cyberattacks discussed in these articles are denial of service, recognition, and distributed denial of service (Freq.). The table also classifies cyberattacks according to STRIDE, which shows that most research in this field has focused on denial of service. On the other hand, many cyber-attacks are spoofing, but not as often. Due to the length of the table, 44 cyberattacks with a frequency of one are not shown. It is appreciated that the vast majority of research has focused on the detection of attacks focused on denial of service. This is consistent with the great destructive impact that these types of attacks have had in recent years.

4.6. RQ6: What are the research gaps and future challenges Anomaly Detection of Cyberattacks for smart homes?

The creation of datasets containing a variety of devices, human interaction, and cyber attacks is one of the most frequently cited difficulties in the selected studies. Datasets containing an heterogeneous number of smart devices is required [89,110,118,168,168]. Moreover, one that reflects the real environment of a smart home, where normal data will be superior to abnormal data and representatives features [160,164]. These datasets should be built over long periods to reflect the normal change in user behavior [98,184]. In addition, datasets should reflect the different smart home topologies, with different numbers of people [124,152], and several behaviors. Finally, they need to present a representative set of cyberattacks [100,104,162]. As a result, these datasets should allow the evaluated models to be implemented in real-world environments without setbacks.

Precisely, deploying the models to a real environment is one of the challenges most mentioned by researchers [89,94,116,162,180]. Several researchers are even interested in testing their models in environments other than the smart home (e.g., industrial IoT, health care, transportation) [107,176]. Moreover, some others propose to evaluate their models on an smart city scale [117], using distributed schemes in several layers and with a large number of smart homes [172].

Several articles indicate the need to profile the normal behavior of devices [107]. With this, models would be able to detect out-of-the-ordinary behavior of these devices and therefore detect potential (even unknown) attacks [168,180]. Moreover, in [112] indicates that IoT devices are so specific that their normal behavior is predictable, so it should be possible to know when they are under attack.

Table 7
Cyberattacks and their STRIDE taxonomy classification.

Cyberattack	Freq.	Used by
DoS or Flooding	63	[90,91,93,94,96–100,102–104,106,108–111,113,115–117,120,123,125–133,137–139,141,143,144,146,148,149,151–153,157–162,164,170–177,179,182–184]
Probing, Reconnaissance or Scan	46	[99,104,108,109,111,113,116,117,123,125,127–129,131,133,139,141,143–149,151,157–159,161,162,164,167,168,170–177,179,180,182–184]
DDoS	33	[89,92,94,97,105–107,109,110,115,116,121,123,127,129,130,132,138,140,141,145–147,152,155,159–162,165,168,171,173]
Botnet	26	[91,94,99,111,112,115,117,118,127,128,131,133,144,145,150–152,157,159,160,165,168,179,180,183,184]
MITM	23	[91,92,99,102,111,113,116,117,125,127,131,133,141,151,157–159,162,169,176,178,179,183]
Brute Force	16	[113,125,127,140,144,152,159,165,172,175,177,179,180,182–184]
Spoofing	13	[101,106,113,116,126,141,159,171,172,176,176,179,183]
Injection	10	[98,103,119,132,147,152,162,176,181,184]
Data Exfiltration or Information theft	19	[116,121,123,129,137,139,141,143,149,159,161,162,164,166,171,173,174,179,180]
Backdoor	7	[147,151,159,170,173,177,181]
User Anomalous Behavior	7	[88,103,122,124,135,148,154,156]
Jamming	5	[90,96,119,132,163]
Deauth attack	4	[102,119,163,180]
Replay	4	[92,95,98,132]
Worm	4	[151,170,173,177]
Fuzzer	4	[151,170,173,177]
Exploit	4	[151,170,173,177]
User to root	3	[108,109,184]
Remote to Local	3	[108,109,184]
Sensor Misuse	3	[88,150,154]
Insecure Firmware	3	[116,132,141]
Ransomware	3	[159,162,180]
Sinkhole attack	2	[95,101]
KeyLogging	2	[127,162]
Impersonation attack	2	[98,103]
Delay attack	2	[90,98]

The researchers aim for their proposed models is to recognize a good variety of attacks and even unknown ones [97,105,107,117,123,146,180]. On the one hand, recognizing unknown attacks in a short window of time would help mitigate their effects quickly [123]. On the other hand, given the use of machine learning techniques to detect IDS attacks, attackers have started to use adversarial machine learning techniques to avoid detection. Given this, the researchers also explain the need to detect these types of attacks [118,119]. Utilizing additional machine learning models to enhance the ability to detect attacks is one of the most frequently cited future projects among researchers [123,160,162,164,166]. Among the techniques mentioned are those of machine learning (especially unsupervised) [124,125]. For example, the use of unsupervised methods to detect unknown attacks is proposed [144,168]. On the other hand, despite the great need for processing resources, several articles mention deep learning methods as future work [89,116,127,129,178]. On the other hand, combining several methods to improve the detection rate is also a potential improvement [180].

Other challenges that appear in the articles of the present review are:

- Evaluate transfer techniques for learning models created for other environments [112].
- Utilize models in a Software-Defined-Network (SDN) environment [117,118].
- Evaluate proposed models on additional datasets [125].
- Utilize network and application layer characteristics to construct detection models [168].
- Employ lightweight procedures [96].
- Anonymize data to protect household confidentiality [156].
- Utilize additional features (not just network-based) [102,168].

- Build adaptive models [102,162].

5. Discussion

This section analyzes the potential research directions identified by this review. Because of the unique context of a smart home, it is essential to develop an architecture for detecting cyberattacks that takes privacy into account. Also, it is essential to make new datasets with new characteristics that consider how a smart home environment is changing.

5.1. Architecture

Defining an IDS smart home architecture with adaptability, no user intervention, multi-user, scalability, real-time usage, lightweight, and high performance in detecting old and zero-day cyberattacks is a big challenge. Smart homes have dynamic environments that must be considered in classification models; these must incorporate new insights based on these changes. On the one hand, the inhabitants of smart homes, over time, modify or acquire new behaviors. On the other hand, zero-day attacks change and evolve to evade new security mechanisms and security patches. In addition, zero-day attacks must be detected in a short time, as they could cause significant damage to an organization in an instant. Therefore, data processing must be commensurate with the capacity of the devices. Indeed, smart homes are places with low-performance hardware, moreover, data must be collected, analyzed, and sorted with low processing capacity. However, a centralized device with better resources and technologies (e.g., fog computing) could be considered to consolidate data and improve sensing performance.

5.2. Classification methods

In recent years, methods associated with DL have been evaluated in smart home contexts. However, caution must be taken since smart home environments have devices with low processing power, a necessary feature for executing these methods. Fog computing has been used to free constrained devices and centralize the computational load on a fog device. Yet, attacks occurring inside the networks could be overlooked.

5.3. Smart home features

The characteristics used by researchers to characterize a smart home come mostly from network traffic. Few articles have been found that focus on the context-specific characteristics of a smart home. Therefore, a challenge is to find relevant features to model normal and malicious behavior and possible variants.

5.4. Privacy

Anomaly detection techniques require large amounts of data to generate models and may contain sensitive data. According to international regulations and standards [204], privacy is an indispensable feature of an IDS system that potentially collects sensitive data. Moreover, the data must be collected with sensors implemented throughout the smart home; therefore, the data can be highly sensitive about its inhabitants. For example, a robot vacuum cleaner could collect information about the house's composition, and detection sensors can infer the hours the house is empty, etc. However, many of the evaluated articles generally mention privacy as a relevant feature when building an IDS, but few care about it. Therefore, the protection of this data must be considered in the development of IDSs. For example, include privacy measures such as encryption, anonymization, pseudo-anonymization, and privacy by design.

5.5. Smart home datasets

Researchers often use their datasets to evaluate their proposals. On the one hand, these datasets have little diversity of cyberattacks (anomalous data). On the other hand, they have little or no interaction with people and between the devices themselves (normal data). Moreover, many articles do not report whether or not there is an interaction between people and devices. Furthermore, the availability of the dataset for reproducibility of the experiments is not reported either. Therefore, it is required to have a publicly accessible dataset consolidated with data from one or several real smart homes with a wide variety of classified attacks. In addition, this dataset must have real people interacting with the devices and each other. In a smart home environment, people change their behaviors. There are discrepancies between the definition of smart homes and the content of the datasets in the reviewed studies. In particular, the articles indicate a smart home setting; however, their experiments are conducted with a small number of IoT devices and minimal human interaction. Current datasets and classification models may work very well at the time of assessment, but in the short, medium and long term they may become obsolete, increasing their false positives. Therefore, it is necessary for the new generation of datasets to take into account that people in a smart home environment are changing their tastes, needs, actions and interactions with different devices. Consequently, new datasets need to be generated over long periods with real people.

5.6. Changing environment

Smart home environments experience continuous change and adaptation due to shifting user behaviors, preferences, and interactions with multiple devices. Consequently, anomaly detection systems (ADS) must remain flexible and responsive to these variations in order to sustain their effectiveness. The authors propose the application of incremental, unsupervised, transfer, and reinforcement learning to develop more adaptable and resilient ADS that are better equipped to handle the dynamic nature of smart homes. These strategies can potentially enhance ADS performance while addressing the obstacles presented by the ever-evolving smart home setting. Incremental learning (online learning) acquires relevant knowledge from incoming data continuously while not needing to access the initial data. In incremental learning, incoming data distribution is unknown and has a highly different probability from the original one. A model must be flexible to acquire new knowledge and stable to consolidate the old one. The goal of incremental learning is to achieve these characteristics and get low processing requirements and improve or preserve classification over time [205]. Therefore, incremental learning is necessary to build an ADS that adapts to dynamics and changing environments, such as a smart home. Other learning techniques, including unsupervised, transfer, and reinforcement learning, can be explored to address the evolving circumstances in smart homes. Unsupervised learning, which does not depend on labeled data, is well-suited for situations with limited or constantly changing data. Transfer learning allows models to utilize the knowledge acquired in one area and apply it to another, offering an efficient means of adapting to new situations without the need for extensive retraining. Reinforcement learning allows models to learn through interaction with their surroundings, obtaining feedback in the form of rewards or penalties, and modifying their behavior as needed. These learning methods have the potential to provide more flexible and resilient solutions for the ever-changing nature of smart home settings, ultimately enhancing the performance of anomaly detection systems.

5.7. Zero-days cyberattacks

Although one of the strengths of using anomaly-based cyberattack detection is the ability to find unknown attacks, very few articles evaluate the ability of the models to classify a zero-day attack as an anomaly. Instead, most of the articles focus on testing the detection of attacks within the same categories of trained attacks. In contrast, some articles assume that the anomalies are direct cyberattacks. However, these anomalies could be device malfunctioning (e.g. low battery), a change in the behavior of an inhabitant, or a new one, among others. Failure to consider these problems could mean an increase in false positives.

6. Conclusion

Research into anomaly-based cyberattack detection systems has increased significantly in recent years. ADS has excellent potential to identify different types of cyberattacks in a smart home context. Furthermore, with the development of telecommuting, detecting known and unknown cyberattacks targeted at the smart home is relevant and can prevent several cyber threats. This paper has presented a careful study of the recent research in ADS on intelligent home environments and its detection, placement, and validation strategies, source of features, datasets, type of anomaly data, evaluation metrics, and open issues. Also, existing taxonomies for anomaly detection and machine learning had to be changed to fit the cyberattack detection methods in the SLR-selected papers. New studies on smart home intrusion detection systems must consider the specific characteristics of these environments: multiple inhabitants, changing behavior over time, devices interacting with each other, configuration and management of devices in the cloud through mobile devices, a lack of knowledge of the application of security measures, among others. Also, users of smart homes will not care if the IDS can find the most recent attacks or if the firmware on their home devices is up to date, so IDS and related architectures must consider these things.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgments

This work was partially funded by the Spanish Ministry of Science and Innovation through project PID2021-125962OB-C31 “SECURING”.

References

[1] F. Dahlqvist, M. Patel, A. Rajko, J. Shulman, Growing opportunities in the Internet of Things, McKinsey & Company, 2019, pp. 1–6.

[2] R. Singh, H. Kumar, R.K. Singla, R.R. Ketti, Internet attacks and intrusion detection system: A review of the literature, Online Inform. Rev. 41 (2) (2017) 171–184, http://dx.doi.org/10.1108/OIR-12-2015-0394.

[3] A. Chatterjee, B.S. Ahmed, IoT anomaly detection methods and applications: A survey, Internet Things 19 (2022) 100568, Publisher: Elsevier.

[4] L. Jiang, D.-Y. Liu, B. Yang, Smart home research, in: Proceedings of 2004 International Conference on Machine Learning and Cybernetics (IEEE Cat. No.04EX826), Vol. 2, 2004, pp. 659–663, http://dx.doi.org/10.1109/ICMLC.2004.1382266.

[5] B.K. Sovacool, D.D. Furszyfer Del Rio, Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies, Renew. Sustain. Energy Rev. 120 (2020) 109663, http://dx.doi.org/10.1016/j.rser.2019.109663, URL http://www.sciencedirect.com/science/article/pii/S1364032119308688.

[6] D. Mocrii, Y. Chen, P. Musilek, IoT-based smart homes: A review of system architecture, software, communications, privacy and security, Internet Things 1–2 (2018) 81–98, http://dx.doi.org/10.1016/j.iot.2018.08.009, URL http://www.sciencedirect.com/science/article/pii/S2542660518300477.

[7] R. Derbyshire, B. Green, D. Prince, A. Mauthe, D. Hutchison, An analysis of cyber security attack taxonomies, in: 2018 IEEE European Symposium on Security and Privacy Workshops, EuroS&PW, IEEE, 2018, pp. 153–161.

[8] V. Sklyar, V. Kharchenko, ENISA documents in cybersecurity assurance for industry 4.0: IIoT threats and attacks scenarios, in: 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Vol. 2, IDAACS, IEEE, 2019, pp. 1046–1049.

[9] Y. Shah, S. Sengupta, A survey on classification of cyber-attacks on IoT and IIoT devices, in: 2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, UEMCON, IEEE, 2020, pp. 0406–0413.

[10] S. Khanam, I.B. Ahmedy, M.Y.I. Idris, M.H. Jaward, A.Q.B.M. Sabri, A survey of security challenges, attacks taxonomy and advanced countermeasures in the Internet of Things, IEEE Access 8 (2020) 219709–219743, Publisher: IEEE.

[11] A. Djenna, D.E. Saïdouni, Cyber attacks classification in IoT-based-healthcare infrastructure, in: 2018 2nd Cyber Security in Networking Conference, CSNet, IEEE, 2018, pp. 1–4.

[12] R. Heartfield, G. Loukas, S. Budimir, A. Bezemskij, J.R. Fontaine, A. Filippoupolitis, E. Roesch, A taxonomy of cyber-physical threats and impact in the smart home, Comput. Secur. 78 (2018) 398–428, Publisher: Elsevier.

[13] M. Howard, S. Lipner, The Security Development Lifecycle, Vol. 8, Microsoft Press Redmond, 2006.

[14] R. Khan, K. McLaughlin, D. Laverty, S. Sezer, STRIDE-based threat modeling for cyber-physical systems, in: 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe, ISGT-Europe, IEEE, 2017, pp. 1–6.

[15] M. Cagnazzo, M. Hertlein, T. Holz, N. Pohlmann, Threat modeling for mobile health systems, in: 2018 IEEE Wireless Communications and Networking Conference Workshops, WCNCW, 2018, pp. 314–319, http://dx.doi.org/10.1109/WCNCW.2018.8369033.

[16] J. Sanfilippo, T. Abegaz, B. Payne, A. Salimi, STRIDE-based threat modeling for MySQL databases, in: K. Arai, R. Bhatia, S. Kapoor (Eds.), Proceedings of the Future Technologies Conference, FTC 2019, in: Advances in Intelligent Systems and Computing, Springer International Publishing, Cham, 2020, pp. 368–378, http://dx.doi.org/10.1007/978-3-030-32523-7_25.

[17] A. Omotosho, B. Ayemlo Haruna, O. Mikail Olaniyi, Threat modeling of Internet of Things health devices, J. Appl. Secur. Res. 14 (1) (2019) 106–121, http://dx.doi.org/10.1080/19361610.2019.1545278, Publisher: Routledge.

[18] M.N. Anwar, M. Nazir, A.M. Ansari, Modeling security threats for smart cities: A STRIDE-based approach, in: S. Ahmed, S.M. Abbas, H. Zia (Eds.), Smart Cities—Opportunities and Challenges, in: Lecture Notes in Civil Engineering, Springer, Singapore, 2020, pp. 387–396, http://dx.doi.org/10.1007/978-981-15-2545-2_33.

[19] E.A. AbuEmera, H.A. ElZouka, A.A. Saad, Security framework for identifying threats in smart manufacturing systems using STRIDE approach, in: 2022 2nd International Conference on Consumer Electronics and Computer Engineering, ICCECE, 2022, pp. 605–612, http://dx.doi.org/10.1109/ICCECE54139.2022.9712770.

[20] S.G. Abbas, S. Zahid, F. Hussain, G.A. Shah, M. Husnain, A threat modelling approach to analyze and mitigate botnet attacks in smart home use case, in: 2020 IEEE 14th International Conference on Big Data Science and Engineering, BigDataSE, 2020, pp. 122–129, http://dx.doi.org/10.1109/BigDataSE50710.2020.00024.

[21] J.J. Cho, M. Kang, Threat modeling analysis on FireStormcx's webcam system, in: 2022 24th International Conference on Advanced Communication Technology, ICACT, 2022, pp. 276–281, http://dx.doi.org/10.23919/ICACT53585.2022.9728974, ISSN: 1738-9445.

[22] R. Zhu, X. Wu, J. Sun, Z. Li, Research on smart home security threat modeling based on STRIDE-IAHP-BN, in: 2021 20th International Symposium on Distributed Computing and Applications for Business Engineering and Science, DCABES, 2021, pp. 207–213, http://dx.doi.org/10.1109/DCABES52998.2021.00059, ISSN: 2473-3636.

[23] D. Sattar, A.H. Vasoukolaei, P. Crysdale, A. Matrawy, A STRIDE threat model for 5G core slicing, in: 2021 IEEE 4th 5G World Forum, 5GWF, 2021, pp. 247–252, http://dx.doi.org/10.1109/5GWF52925.2021.00050.

[24] M.D. Furtado, R.D. Mushrall, H. Liu, Threat analysis of the security credential management system for vehicular communications, in: 2018 IEEE International Symposium on Technologies for Homeland Security, HST, 2018, pp. 1–5, http://dx.doi.org/10.1109/THS.2018.8574206.

[25] D. Geneiatakis, I. Kounelis, R. Neisse, I. Nai-Fovino, G. Steri, G. Baldini, Security and privacy issues for an IoT based smart home, in: 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO, 2017, pp. 1292–1297, http://dx.doi.org/10.23919/MIPRO.2017.7973622.

[26] J.C. Sapalo Sicato, P.K. Sharma, V. Loia, J.H. Park, VPNFilter malware analysis on cyber threat in smart home network, Appl. Sci. 9 (13) (2019) 2763, http://dx.doi.org/10.3390/app9132763, Number: 13 Publisher: Multidisciplinary Digital Publishing Institute URL https://www.mdpi.com/2076-3417/9/13/2763.

[27] Nmap: The Network Mapper - Free Security Scanner, URL https://nmap.org/.

[28] U. Saxena, J. Sodhi, Y. Singh, An analysis of DDoS attacks in a smart home networks, in: 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2020, pp. 272–276, http://dx.doi.org/10.1109/Confluence47617.2020.9058087.

[29] B. Tushir, Y. Dalal, B. Dezfouli, Y. Liu, A quantitative study of DDoS and E-DDoS attacks on WiFi smart home devices, IEEE Internet Things J. 8 (8) (2021) 6282–6292, http://dx.doi.org/10.1109/JIOT.2020.3026023, Conference Name: IEEE Internet of Things Journal.

[30] Famous DDoS attacks | Biggest DDoS attacks, Cloudflare, URL https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/.

[31] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J.A. Halderman, L. Invernizzi, M. Kallitsis, Understanding the mirai botnet, in: 26th $USENIX$ Security Symposium ($USENIX$, Security 17, 2017, pp. 1093–1110.

[32] Hacker Compromised Family's Wi-Fi, Taunted Family With Thermostat, Camera for 24 Hours - Security News, URL https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hacker-compromised-family-s-wi-fi-taunted-family-with-thermostat-camera-for-24-hours.

[33] What is a Zero-day Attack? - Definition and Explanation, Www.Kaspersky.Com, 2022, Section: Resource Center URL https://www.kaspersky.com/resource-center/definitions/zero-day-exploit.

[34] M. Labs, Worms Could Spread Like Zombies via Internet of Things, McAfee Blog, 2016, URL https://www.mcafee.com/blogs/other-blogs/mcafee-labs/worms-could-spread-like-zombies-via-internet-of-things/.

[35] Fuzzers - an overview | ScienceDirect Topics, URL https://www.sciencedirect.com/topics/computer-science/fuzzers.

[36] C.K. Nkuba, S. Kim, S. Dietrich, H. Lee, Riding the IoT wave with VFuzz: Discovering security flaws in smart homes, IEEE Access 10 (2021) 1775–1789, Publisher: IEEE.

[37] Qué es una Puerta Trasera - Panda Security, URL https://www.pandasecurity.com/.

[38] S. Hashemi, M. Zarei, Internet of Things backdoors: Resource management issues, security challenges, and detection methods, Trans. Emerg. Telecommun. Technol. 32 (2) (2021) e4142, http://dx.doi.org/10.1002/ett.4142, URL https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.4142.

[39] Exploit, definición y características - Panda Security, URL https://www.pandasecurity.com/.

[40] T.A. Abdullah, W. Ali, S. Malebary, A.A. Ahmed, A review of cyber security challenges attacks and solutions for Internet of Things based smart home, Int. J. Comput. Sci. Netw. Secur. 19 (9) (2019) 139.

[41] KDD Cup 1999 Data, KDD Cup 1999 Data, URL http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[42] R. Cheema, D. Bansal, S. Sofat, Deauthentication/disassociation attack: Implementation and security in wireless mesh networks, Int. J. Comput. Appl. 23 (7) (2011) 7–15, Publisher: Citeseer.

[43] A.C. Jose, R. Malekian, Smart home automation security: A literature review, SmartCR 5 (4) (2015) 269–285.

[44] H. Chi, C. Fu, Q. Zeng, X. Du, Delay wreaks havoc on your smart home: Delay-based automation interference attacks, in: 2022 IEEE Symposium on Security and Privacy, SP, 2022, pp. 285–302, http://dx.doi.org/10.1109/SP46214.2022.9833620, ISSN: 2375-1207.

[45] M. Humayun, N. Jhanjhi, A. Alsayat, V. Ponnusamy, Internet of Things and ransomware: Evolution, mitigation and prevention, Egypt. Inform. J. 22 (1) (2021) 105–117, http://dx.doi.org/10.1016/j.eij.2020.05.003, URL https://www.sciencedirect.com/science/article/pii/S1110866520301304.

[46] M.F. Elrawy, A.I. Awad, H.F.A. Hamed, Intrusion detection systems for IoT-based smart environments: A survey, J. Cloud Comput. 7 (1) (2018) 21, http://dx.doi.org/10.1186/s13677-018-0123-6.

[47] A. Le, J. Loo, Y. Luo, A. Lasebae, Specification-based IDS for securing RPL from topology attacks, in: 2011 IFIP Wireless Days, WD, 2011, pp. 1–3, http://dx.doi.org/10.1109/WD.2011.6098218.

[48] A. Khraisat, A. Alazab, A critical review of intrusion detection systems in the Internet of Things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges, Cybersecurity 4 (1) (2021) 18, http://dx.doi.org/10.1186/s42400-021-00077-7.

[49] K.G. Mehrotra, C.K. Mohan, H. Huang, Anomaly Detection Principles and Algorithms, Vol. 1, Springer, 2017.

[50] V. Chandola, A. Banerjee, V. Kumar, Anomaly detection: A survey, ACM Comput. Surv. 41 (3) (2009) 15:1–15:58, http://dx.doi.org/10.1145/1541880.1541882.

[51] A.B. Nassif, M.A. Talib, Q. Nasir, F.M. Dakalbab, Machine learning for anomaly detection: A systematic review, Ieee Access 9 (2021) 78658–78700, Publisher: IEEE.

[52] A. Patcha, J.-M. Park, An overview of anomaly detection techniques: Existing solutions and latest technological trends, Comput. Netw. 51 (12) (2007) 3448–3470, http://dx.doi.org/10.1016/j.comnet.2007.02.001, URL https://www.sciencedirect.com/science/article/pii/S138912860700062X.

[53] M.H. Bhuyan, D.K. Bhattacharyya, J.K. Kalita, Network anomaly detection: Methods, systems and tools, IEEE Commun. Surv. Tutor. 16 (1) (2014) 303–336, http://dx.doi.org/10.1109/SURV.2013.052213.00046, Conference Name: IEEE Communications Surveys & Tutorials.

[54] M. Ahmed, A. Naser Mahmood, J. Hu, A survey of network anomaly detection techniques, J. Netw. Comput. Appl. 60 (2016) 19–31, http://dx.doi.org/10.1016/j.jnca.2015.11.016, URL https://www.sciencedirect.com/science/article/pii/S1084804515002891.

[55] R. Makani, B.V.R. Reddy, Taxonomy of machine leaning based anomaly detection and its suitability, Procedia Comput. Sci. 132 (2018) 1842–1849, Publisher: Elsevier.

[56] R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, Machine learning models for secure data analytics: A taxonomy and threat model, Comput. Commun. 153 (2020) 406–440, Publisher: Elsevier.

[57] B. Kitchenham, S. Charters, Guidelines for performing systematic literature reviews in software engineering, 2007.

[58] B.B. Zarpelão, R.S. Miani, C.T. Kawakani, S.C. de Alvarenga, A survey of intrusion detection in Internet of Things, J. Netw. Comput. Appl. 84 (2017) 25–37, http://dx.doi.org/10.1016/j.jnca.2017.02.009, URL http://www.sciencedirect.com/science/article/pii/S1084804517300802.

[59] M.A. Al-Garadi, A. Mohamed, A.K. Al-Ali, X. Du, I. Ali, M. Guizani, A survey of machine and deep learning methods for Internet of Things (IoT) security, IEEE Commun. Surv. Tutor. 22 (3) (2020) 1646–1685, http://dx.doi.org/10.1109/COMST.2020.2988293.

[60] F. Hussain, R. Hussain, S.A. Hassan, E. Hossain, Machine learning in IoT security: Current solutions and future challenges, IEEE Commun. Surv. Tutor. 22 (3) (2020) 1686–1721, http://dx.doi.org/10.1109/COMST.2020.2986444.

[61] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, J. Lopez, A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3453–3495, http://dx.doi.org/10.1109/COMST.2018.2855563, Conference Name: IEEE Communications Surveys & Tutorials.

[62] M.A. Amanullah, R.A.A. Habeeb, F.H. Nasaruddin, A. Gani, E. Ahmed, A.S.M. Nainar, N.M. Akim, M. Imran, Deep learning and big data technologies for IoT security, Comput. Commun. 151 (2020) 495–517, http://dx.doi.org/10.1016/j.comcom.2020.01.016, URL http://www.sciencedirect.com/science/article/pii/S0140366419315361.

[63] E. Benkhelifa, T. Welsh, W. Hamouda, A critical review of practices and challenges in intrusion detection systems for IoT: Toward universal and resilient systems, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3496–3509, http://dx.doi.org/10.1109/COMST.2018.2844742.

[64] S. Hajiheidari, K. Wakil, M. Badri, N.J. Navimipour, Intrusion detection systems in the Internet of things: A comprehensive investigation, Comput. Netw. 160 (2019) 165–191, http://dx.doi.org/10.1016/j.comnet.2019.05.014, URL https://www.sciencedirect.com/science/article/pii/S1389128619306267.

[65] J.M. Batalla, A. Vasilakos, M. Gajewski, Secure smart homes: Opportunities and challenges, ACM Comput. Surv. 50 (5) (2017) 1–32, Publisher: ACM New York, NY, USA.

[66] J. Asharf, N. Moustafa, H. Khurshid, E. Debie, W. Haider, A. Wahab, A review of intrusion detection systems using machine and deep learning in Internet of Things: Challenges, solutions and future directions, Electronics 9 (7) (2020) 1177, Publisher: MDPI.

[67] M. Fahim, A. Sillitti, Anomaly detection, analysis and prediction techniques in iot environment: A systematic literature review, IEEE Access 7 (2019) 81664–81681, Publisher: IEEE.

[68] A. Thakkar, R. Lohiya, A review on machine learning and deep learning perspectives of IDS for IoT: Recent updates, security issues, and challenges, Arch. Comput. Methods Eng. 28 (4) (2021) 3211–3243, Publisher: Springer.

[69] N. Mishra, S. Pandya, Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review, IEEE Access 9 (2021) 59353–59377, Publisher: IEEE.

[70] Z.A. Khan, P. Herrmann, J.M. Alcaraz-Calero, Recent advancements in intrusion detection systems for the Internet of Things, Secur. Commun. Netw. 2019 (2019) http://dx.doi.org/10.1155/2019/4301409.

[71] A. Tabassum, A. Erbad, M. Guizani, A survey on recent approaches in intrusion detection system in iots, in: 2019 15th International Wireless Communications & Mobile Computing Conference, IWCMC, IEEE, 2019, pp. 1190–1197.

[72] S.H. Haji, S.Y. Ameen, Attack and anomaly detection in iot networks using machine learning techniques: A review, Asian J. Res. Comput. Sci. 9 (2) (2021) 30–46.

[73] I. Idrissi, M. Azizi, O. Moussaoui, IoT security with deep learning-based intrusion detection systems: A systematic literature review, in: 2020 Fourth International Conference on Intelligent Computing in Data Sciences, ICDS, IEEE, 2020, pp. 1–10.

[74] K. Albulayhi, A.A. Smadi, F.T. Sheldon, R.K. Abercrombie, IoT intrusion detection taxonomy, reference architecture, and analyses, Sensors 21 (19) (2021) 6432, Publisher: MDPI.

[75] A. Diro, N. Chilamkurti, V.-D. Nguyen, W. Heyne, A comprehensive study of anomaly detection schemes in IoT networks using machine learning algorithms, Sensors 21 (24) (2021) 8320, Publisher: MDPI.

[76] B. Hammi, S. Zeadally, R. Khatoun, J. Nebhen, Survey on smart homes: Vulnerabilities, risks, and countermeasures, Comput. Secur. 117 (2022) 102677, Publisher: Elsevier.

[77] A. Qureshi, M.A. Qureshi, H.A. Haider, R. Khawaja, A review on machine learning techniques for secure IoT networks, in: 2020 IEEE 23rd International Multitopic Conference, INMIC, IEEE, 2020, pp. 1–6.

[78] M. Albany, E. Alsahafi, I. Alruwili, S. Elkhediri, A review: Secure Internet of Thing system for smart houses, Procedia Comput. Sci. 201 (2022) 437–444, Publisher: Elsevier.

[79] A.F. Jahwar, S.R. Zeebaree, A state of the art survey of machine learning algorithms for IoT security, Asian J. Res. Comput. Sci (2021) 12–34.

[80] P. Gupta, L. Yadav, D.S. Tomar, Internet of Things: A Review on Machine Learning-based Intrusion Detection System.

[81] J. Yu, A. de Antonio, E. Villalba-Mora, Deep learning (CNN, RNN) applications for smart homes: A systematic review, Computers 11 (2) (2022) 26, Publisher: MDPI.

[82] P. Kumar, G.P. Gupta, R. Tripathi, A Review on Intrusion Detection System and Cyber Threat Intelligence for Secure IoT-enabled Network: Challenges and Directions.

[83] A.A. Anitha, L. Arockiam, A Review on Intrusion Detection Systems to Secure IoT Networks.

[84] Z. Wang, D. Liu, Y. Sun, X. Pang, P. Sun, F. Lin, J.C. Lui, K. Ren, A survey on IoT-enabled home automation systems: Attacks and defenses, IEEE Commun. Surv. Tutor. (2022) Publisher: IEEE.

[85] R. Balaji, S. Deepajothi, G. Prabaharan, T. Daniya, P. Karthikeyan, S. Velliangiri, Survey on intrusions detection system using deep learning in IoT environment, in: 2022 International Conference on Sustainable Computing and Data Communication Systems, ICSCDS, IEEE, 2022, pp. 195–199.

[86] P. Brereton, B.A. Kitchenham, D. Budgen, M. Turner, M. Khalil, Lessons from applying the systematic literature review process within the software engineering domain, J. Syst. Softw. 80 (4) (2007) 571–583, http://dx.doi.org/10.1016/j.jss.2006.07.009, URL https://www.sciencedirect.com/science/article/pii/S016412120600197X.

[87] S. Aldhaheri, D. Alghazzawi, L. Cheng, A. Barnawi, B.A. Alzahrani, Artificial immune systems approaches to secure the Internet of Things: A systematic review of the literature and recommendations for future research, J. Netw. Comput. Appl. 157 (2020) 102537, http://dx.doi.org/10.1016/j.jnca.2020.102537, URL http://www.sciencedirect.com/science/article/pii/S1084804520300114.

[88] M. Nobakht, V. Sivaraman, R. Boreli, A host-based intrusion detection and mitigation framework for smart home IoT using OpenFlow, in: 2016 11th International Conference on Availability, Reliability and Security, ARES, 2016, pp. 147–156, http://dx.doi.org/10.1109/ARES.2016.64.

[89] Y. Al Mtawa, H. Singh, A. Haque, A. Refaey, Smart home networks: Security perspective and ML-based DDoS detection, in: 2020 IEEE Canadian Conference on Electrical and Computer Engineering, CCECE, 2020, pp. 1–8, http://dx.doi.org/10.1109/CCECE47787.2020.9255756, ISSN: 2576-7046.

[90] B. Al Baalbaki, J. Pacheco, C. Tunc, S. Hariri, Y. Al-Nashif, Anomaly behavior analysis system for ZigBee in smart buildings, in: 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications, AICCSA, IEEE, 2015, pp. 1–4.

[91] Z. Liu, N. Thapa, A. Shaver, K. Roy, X. Yuan, S. Khorsandroo, Anomaly detection on IoT network intrusion using machine learning, in: 2020 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems, IcABCD, 2020, pp. 1–5, http://dx.doi.org/10.1109/icABCD49160.2020.9183842.

[92] A. Kanev, A. Nasteka, C. Bessonova, D. Nevmerzhitsky, A. Silaev, A. Efremov, K. Nikiforova, Anomaly detection in wireless sensor network of the "smart home" system, in: 2017 20th Conference of Open Innovations Association, FRUCT, 2017, pp. 118–124, http://dx.doi.org/10.23919/FRUCT.2017.8071301, ISSN: 2305-7254.

[93] J. Pacheco, V.H. Benitez, L.C. Félix-Herrán, P. Satam, Artificial neural networks-based intrusion detection system for Internet of Things Fog nodes, IEEE Access 8 (2020) 73907–73918, http://dx.doi.org/10.1109/ACCESS.2020.2988055, Conference Name: IEEE Access.

[94] S.S. Bhunia, M. Gurusamy, Dynamic attack detection and mitigation in IoT using SDN, in: 2017 27th International Telecommunication Networks and Applications Conference, ITNAC, 2017, pp. 1–6, http://dx.doi.org/10.1109/ATNAC.2017.8215418, ISSN: 2474-154X.

[95] G. Tertytchny, N. Nicolaou, M.K. Michael, Classifying network abnormalities into faults and attacks in IoT-based cyber physical systems using machine learning, Microprocess. Microsyst. 77 (2020) 103121, http://dx.doi.org/10.1016/j.micpro.2020.103121, URL https://www.sciencedirect.com/science/article/pii/S014193312030288X.

[96] D. Midi, A. Rullo, A. Mudgerikar, E. Bertino, Kalis — A system for knowledge-driven adaptable intrusion detection for the Internet of Things, in: 2017 IEEE 37th International Conference on Distributed Computing Systems, ICDCS, 2017, pp. 656–666, http://dx.doi.org/10.1109/ICDCS.2017.104, ISSN: 1063-6927.

[97] J. Galeano-Brajones, J. Carmona-Murillo, J.F. Valenzuela-Valdés, F. Luna-Valero, Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: An experimental approach, Sensors 20 (3) (2020) http://dx.doi.org/10.3390/s20030816, URL https://www.mdpi.com/1424-8220/20/3/816.

[98] J. Pacheco, S. Hariri, Anomaly behavior analysis for IoT sensors, Trans. Emerg. Telecommun. Technol. 29 (4) (2018) e3188, Publisher: Wiley Online Library.

[99] S.W. Azumah, N. Elsayed, V. Adewopo, Z.S. Zaghloul, C. Li, A deep lstm based approach for intrusion detection iot devices network in smart home, in: 2021 IEEE 7th World Forum on Internet of Things, WF-IoT, IEEE, 2021, pp. 836–841.

[100] O. Brun, Y. Yin, E. Gelenbe, Y.M. Kadioglu, J. Augusto-Gonzalez, M. Ramos, Deep learning with dense random neural networks for detecting attacks against IoT-connected home environments, in: International ISCIS Security Workshop, Springer, Cham, 2018, pp. 79–89.

[101] D.J. Atul, R. Kamalraj, G. Ramesh, K.S. Sankaran, S. Sharma, S. Khasim, A machine learning based IoT for providing an intrusion detection system for security, Microprocess. Microsyst. 82 (2021) 103741, Publisher: Elsevier.

[102] J. Roux, E. Alata, G. Auriol, M. Kaaniche, V. Nicomette, R. Cayre, RadIoT: Radio communications intrusion detection for IoT - a protocol independent approach, in: 2018 IEEE 17th International Symposium on Network Computing and Applications, NCA, 2018, pp. 1–8, http://dx.doi.org/10.1109/NCA.2018.8548286.

[103] A.K. Sikder, L. Babun, A.S. Uluagac, Aegis+ A context-aware platform-independent security framework for smart home systems, Digit. Threats: Res. Pract. 2 (1) (2021) 1–33, Publisher: ACM New York, NY, USA.

[104] C.D. McDermott, F. Majdani, A.V. Petrovski, Botnet detection in the Internet of Things using deep learning approaches, in: 2018 International Joint Conference on Neural Networks, IJCNN, 2018, pp. 1–8, http://dx.doi.org/10.1109/IJCNN.2018.8489489, ISSN: 2161-4407.

[105] N. Alsabilah, D.B. Rawat, Anomaly detection in smart home networks using Kalman filter, in: IEEE INFOCOM 2021-IEEE Conference on Computer Communications Workshops, INFOCOM WKSHPS, IEEE, 2021, pp. 1–6.

[106] P. Bhatt, A. Morais, HADS: Hybrid anomaly detection system for IoT environments, in: 2018 International Conference on Internet of Things, Embedded Systems and Communications, IINTEC, 2018, pp. 191–196, http://dx.doi.org/10.1109/IINTEC.2018.8695303.

[107] I. Cvitić, D. Peraković, B. Gupta, K.-K.R. Choo, Boosting-based DDoS detection in Internet of Things systems, IEEE Internet Things J. (2021) Publisher: IEEE.

[108] K. Liu, Z. Fan, M. Liu, S. Zhang, Hybrid intrusion detection method based on K-means and CNN for smart home, in: 2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems, CYBER, 2018, pp. 312–317, http://dx.doi.org/10.1109/CYBER.2018.8688271, ISSN: 2379-7711.

[109] E. Krishna, T. Arunkumar, Hybrid particle swarm and gray wolf optimization algorithm for IoT intrusion detection system, Int. J. Intell. Eng. Syst. 14 (2021) 66–76, http://dx.doi.org/10.22266/ijies2021.0831.07.
[110] R. Doshi, N. Apthorpe, N. Feamster, Machine learning DDoS detection for consumer Internet of Things devices, in: 2018 IEEE Security and Privacy Workshops, SPW, 2018, pp. 29–35, http://dx.doi.org/10.1109/SPW.2018.00013.
[111] N. Elsayed, Z.S. Zaghloul, S.W. Azumah, C. Li, Intrusion detection system in smart home network using bidirectional LSTM and convolutional neural networks hybrid model, in: 2021 IEEE International Midwest Symposium on Circuits and Systems, MWSCAS, 2021, pp. 55–58, http://dx.doi.org/10.1109/MWSCAS47672.2021.9531683, ISSN: 1558-3899.
[112] Y. Meidan, M. Bohadana, Y. Mathov, Y. Mirsky, A. Shabtai, D. Breitenbacher, Y. Elovici, N-BaIoT—Network-based detection of IoT botnet attacks using deep autoencoders, IEEE Pervasive Comput. 17 (3) (2018) 12–22, http://dx.doi.org/10.1109/MPRV.2018.03367731, Conference Name: IEEE Pervasive Computing.
[113] H. Alkahtani, T.H.H. Aldhyani, Intrusion detection system to advance Internet of Things infrastructure-based deep learning algorithms, in: M.I. Uddin (Ed.), Complexity 2021 (2021) 5579851, http://dx.doi.org/10.1155/2021/5579851, Publisher: Hindawi.
[114] H. Mohammed, T.A. Odetola, S.R. Hasan, S. Stissi, I. Garlin, F. Awwad, (HiadIoT): Hardware intrinsic attack detection in Internet of Things; Leveraging power profiling, in: 2019 Ieee 62nd International Midwest Symposium on Circuits and Systems, Mwscas, IEEE, 2019, pp. 852–855.
[115] R. Abu Khurma, I. Almomani, I. Aljarah, IoT botnet detection using salp swarm and ant Lion hybrid optimization model, Symmetry 13 (8) (2021) http://dx.doi.org/10.3390/sym13081377, URL https://www.mdpi.com/2073-8994/13/8/1377.
[116] E. Anthi, L. Williams, M. Slowinska, G. Theodorakopoulos, P. Burnap, A supervised intrusion detection system for smart home IoT devices, Ieee Internet Things J. 6 (5) (2019) 9042–9053, http://dx.doi.org/10.1109/JIOT.2019.2926365.
[117] J. Ashraf, M. Keshk, N. Moustafa, M. Abdel-Basset, H. Khurshid, A.D. Bakhshi, R.R. Mostafa, IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities, Sustainable Cities Soc. 72 (2021) 103041, http://dx.doi.org/10.1016/j.scs.2021.103041, URL https://www.sciencedirect.com/science/article/pii/S2210670721003255.
[118] M.R. Shahid, G. Blanc, Z. Zhang, H. Debar, Anomalous communications detection in IoT networks using sparse autoencoders, in: 2019 IEEE 18th International Symposium on Network Computing and Applications, NCA, IEEE, 2019, pp. 1–5.
[119] R. Heartfield, G. Loukas, A. Bezemskij, E. Panaousis, Self-configurable cyber-physical intrusion detection for smart homes using reinforcement learning, IEEE Trans. Inf. Forensics Secur. 16 (2021) 1720–1735, http://dx.doi.org/10.1109/TIFS.2020.3042049, Conference Name: IEEE Transactions on Information Forensics and Security.
[120] J. Pacheco, V.H. Benitez, C. Tunc, C. Grijalva, Anomaly behavior analysis for fog nodes availability assurance in IoT applications, in: 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications, AICCSA, 2019, pp. 1–6, http://dx.doi.org/10.1109/AICCSA47632.2019.9035338, ISSN: 2161-5330.
[121] K. Bobrovnikova, S. Lysenko, P.T. Popov, D. Denysiuk, A. Goroshko, Technique for IoT cyberattacks detection based on the energy consumption analysis, in: IntelITSIS?2021: 2nd International Workshop on Intelligent Information Technologies and Systems of Information Security, Vol. 2853, 2021, Journal Abbreviation: CEUR Workshop Proceedings URL https://openaccess.city.ac.uk/id/eprint/26372/.
[122] M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda, Y. Kato, Anomaly detection for smart home based on user behavior, in: 2019 IEEE International Conference on Consumer Electronics, ICCE, 2019, pp. 1–6, http://dx.doi.org/10.1109/ICCE.2019.8661976.
[123] L. Shi, L. Wu, Z. Guan, Three-layer hybrid intrusion detection model for smart home malicious attacks, Comput. Electr. Eng. 96 (2021) 107536, http://dx.doi.org/10.1016/j.compeleceng.2021.107536, URL https://www.sciencedirect.com/science/article/pii/S004579062100481X.
[124] S. Ramapatruni, S.N. Narayanan, S. Mittal, A. Joshi, K. Joshi, Anomaly detection models for smart home security, in: 2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security, IDS, 2019, pp. 19–24, http://dx.doi.org/10.1109/BigDataSecurity-HPSC-IDS.2019.00015.
[125] R. Qaddoura, A.M. Al-Zoubi, I. Almomani, H. Faris, A multi-stage classification approach for IoT intrusion detection based on clustering with oversampling, Appl. Sci. 11 (7) (2021) 3022, http://dx.doi.org/10.3390/app11073022, Number: 7 Publisher: Multidisciplinary Digital Publishing Institute URL https://www.mdpi.com/2076-3417/11/7/3022.
[126] R. Paudel, T. Muncy, W. Eberle, Detecting dos attack in smart home iot devices using a graph-based approach, in: 2019 IEEE International Conference on Big Data (Big Data), IEEE, 2019, pp. 5249–5258.
[127] I. Ullah, Q.H. Mahmoud, Design and development of a deep learning-based model for anomaly detection in IoT networks, IEEE Access 9 (2021) 103906–103926, http://dx.doi.org/10.1109/ACCESS.2021.3094024, Conference Name: IEEE Access.
[128] T.D. Nguyen, S. Marchal, M. Miettinen, H. Fereidooni, N. Asokan, A.-R. Sadeghi, DIoT: A federated self-learning anomaly detection system for IoT, in: 2019 39th Ieee International Conference on Distributed Computing Systems, Icdcs 2019, Ieee Computer Soc, Los Alamitos, 2019, pp. 756–767, http://dx.doi.org/10.1109/ICDCS.2019.00080.
[129] A. Aljumah, IoT-based intrusion detection system using convolution neural networks, PeerJ Comput. Sci. 7 (2021) e721, http://dx.doi.org/10.7717/peerj-cs.721, Publisher: PeerJ Inc. URL https://peerj.com/articles/cs-721.
[130] A. Procopiou, N. Komninos, C. Douligeris, ForChaos: Real time application DDoS detection using forecasting and chaos theory in smart home IoT network, Wirel. Commun. Mob. Comput. 2019 (2019) Publisher: Hindawi.
[131] H. Kumar, A.R. Jadhav, G.V.K. Sasirekha, J. Bapat, D. Das, Intelligent edge detection of attacks on IP-based IoT deployments, in: 2021 19th OITS International Conference on Information Technology, OCIT, IEEE, 2021, pp. 132–137.
[132] V. Subbarayalu, B. Surendiran, P. Arun Raj Kumar, Hybrid network intrusion detection system for smart environments based on Internet of Things, Comput. J. 62 (12) (2019) 1822–1839, http://dx.doi.org/10.1093/comjnl/bxz082.
[133] M. Tawfik, N.M. Al-Zidi, B. Alsellami, A.M. Al-Hejri, S. Nimbhore, Internet of things-based middleware against cyber-attacks on smart homes using software-defined networking and deep learning, in: 2021 2nd International Conference on Computational Methods in Science & Technology, ICCMST, IEEE, 2021, pp. 7–13.
[134] P.K. Sharma, J.H. Park, Y.-S. Jeong, J.H. Park, SHSec: SDN based secure smart home network architecture for Internet of Things, Mob. Netw. Appl. 24 (3) (2019) 913–924, http://dx.doi.org/10.1007/s11036-018-1147-3.
[135] M. Yamauchi, Y. Ohsita, M. Murata, Platform utilizing similar users' data to detect anomalous operation of home IoT without sharing private information, IEEE Access 9 (2021) 130615–130626, Publisher: IEEE.
[136] Y. Zhou, Y. Liu, S. Hu, Smart home cyberattack detection framework for sponsor incentive attacks, IEEE Trans. Smart Grid 10 (2) (2019) 1916–1927, http://dx.doi.org/10.1109/TSG.2017.2781695, Conference Name: IEEE Transactions on Smart Grid.
[137] D. Krishnan, P. Babu, Imbalanced classification for botnet detection in Internet of Things, in: Next Generation of Internet of Things: Proceedings of ICNGIoT 2021, Springer, 2021, pp. 595–605.
[138] S. Wang, K.M. Gomez, K. Sithamparanathan, P. Zanna, Software defined network security framework for IoT based smart home and city applications, in: 2019 13th International Conference on Signal Processing and Communication Systems, ICSPCS, 2019, pp. 1–8, http://dx.doi.org/10.1109/ICSPCS47537.2019.9008703.
[139] N. Amraoui, B. Zouari, Anomalous behavior detection-based approach for authenticating smart home system users, Int. J. Inf. Secur. (2021) 1–26, Publisher: Springer.
[140] M. Dilraj, K. Nimmy, S. Sankaran, Towards behavioral profiling based anomaly detection for smart homes, in: TENCON 2019 - 2019 IEEE Region 10 Conference, TENCON, 2019, pp. 1258–1263, http://dx.doi.org/10.1109/TENCON.2019.8929235.

[141] F.H. Nakagawa, S.B. Junior, B.B. Zarpelao, Attack detection in smart home IoT networks using CluStream and page-Hinkley test, in: 2021 IEEE Latin-American Conference on Communications, LATINCOM, IEEE, 2021, pp. 1–6.
[142] M. Gajewski, J.M. Batalla, A. Levi, C. Togay, C.X. Mavromoustakis, G. Mastorakis, Two-tier anomaly detection based on traffic profiling of the home automation system, Comput. Netw. 158 (2019) 46–60, http://dx.doi.org/10.1016/j.comnet.2019.04.013.
[143] Y. Jia, Y. Cheng, J. Shi, Semi-supervised variational temporal convolutional network for IoT communication multi-anomaly detection, in: Proceedings of the 2022 3rd International Conference on Control, Robotics and Intelligent System, 2022, pp. 67–73.
[144] O. Salman, I.H. Elhajj, A. Chehab, A. Kayssi, A machine learning based framework for IoT device identification and abnormal traffic detection, Trans. Emerg. Telecommun. Technol. 33 (3) (2022) e3743, http://dx.doi.org/10.1002/ett.3743, URL https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3743.
[145] F. He, F. Tong, Y. Zhang, A bi-layer intrusion detection based on device behavior profiling for smart home IoT, in: 2022 IEEE 19th International Conference on Mobile Ad Hoc and Smart Systems, MASS, IEEE, 2022, pp. 373–379.
[146] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, A. Alazab, A novel ensemble of hybrid intrusion detection system for detecting Internet of Things attacks, Electronics 8 (11) (2019) 1210, http://dx.doi.org/10.3390/electronics8111210, Number: 11 Publisher: Multidisciplinary Digital Publishing Institute URL https://www.mdpi.com/2079-9292/8/11/1210.
[147] T. Gazdar, A new IDS for smart home based on machine learning, in: 2022 14th International Conference on Computational Intelligence and Communication Networks, CICN, IEEE, 2022, pp. 393–400.
[148] M. Hasan, M.M. Islam, M.I.I. Zarif, M.M.A. Hashem, Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches, Internet Things 7 (2019) 100059, http://dx.doi.org/10.1016/j.iot.2019.100059, URL http://www.sciencedirect.com/science/article/pii/S2542660519300241.
[149] P.K. Yadav, A. Kumar, Analysis of machine learning model for anomaly and attack detection in IoT devices, in: 2022 4th International Conference on Inventive Research in Computing Applications, ICIRCA, IEEE, 2022, pp. 387–392.
[150] S. Tang, Z. Gu, Q. Yang, S. Fu, Smart home IoT anomaly detection based on ensemble model learning from heterogeneous data, in: 2019 IEEE International Conference on Big Data (Big Data), 2019, pp. 4185–4190, http://dx.doi.org/10.1109/BigData47090.2019.9006249.
[151] C. Diallo, IoT anomaly detection and attack identification using smart traffic classification techniques, in: 2022 7th International Conference on Frontiers of Signal Processing, ICFSP, IEEE, 2022, pp. 51–58.
[152] F. Alghayadh, D. Debnath, A hybrid intrusion detection system for smart home security, in: 2020 IEEE International Conference on Electro Information Technology, EIT, 2020, pp. 319–323, http://dx.doi.org/10.1109/EIT48999.2020.9208296.
[153] T. Oshio, S. Okada, T. Mitsunaga, Machine learning-based anomaly detection in ZigBee networks, in: 2022 IEEE International Conference on Computing, ICOCO, IEEE, 2022, pp. 259–263.
[154] G. Spanos, K.M. Giannoutakis, K. Votis, B. Viaño, J. Augusto-Gonzalez, G. Aivatoglou, D. Tzovaras, A lightweight cyber-security defense framework for smart homes, in: 2020 International Conference on INnovations in Intelligent SysTems and Applications, INISTA, IEEE, 2020, pp. 1–7.
[155] R.R. Das, B. Krishnamurthy, S. Das, Securing IoT devices using ensemble machine learning in smart home management system, in: 2022 IEEE Symposium Series on Computational Intelligence, SSCI, IEEE, 2022, pp. 915–922.
[156] M. Yamauchi, Y. Ohsita, M. Murata, K. Ueda, Y. Kato, Anomaly detection in smart home operation from user behaviors and home conditions, Ieee Trans. Consum. Electron. 66 (2) (2020) 183–192, http://dx.doi.org/10.1109/TCE.2020.2981636.
[157] S. Sohail, Z. Fan, X. Gu, F. Sabrina, Multi-tiered artificial neural networks model for intrusion detection in smart homes, Intell. Syst. Appl. 16 (2022) 200152, Publisher: Elsevier.
[158] P. Maniriho, E. Niyigaba, Z. Bizimana, V. Twiringiyimana, L.J. Mahoro, T. Ahmad, Anomaly-based intrusion detection approach for iot networks using machine learning, in: 2020 International Conference on Computer Engineering, Network, and Intelligent Multimedia, CENIM, IEEE, 2020, pp. 303–308.
[159] M. Baz, SEHIDS: Self evolving host-based intrusion detection system for IoT networks, Sensors 22 (17) (2022) 6505, Publisher: MDPI.
[160] M. Mafarja, A.A. Heidari, M. Habib, H. Faris, T. Thaher, I. Aljarah, Augmented whale feature selection for IoT attacks: Structure, analysis and applications, Future Gener. Comput. Syst. 112 (2020) 18–40, Publisher: Elsevier.
[161] J.G. Almaraz-Rivera, J.A. Perez-Diaz, J.A. Cantoral-Ceballos, Transport and application layer DDoS attacks detection to IoT devices by using machine learning and deep learning models, Sensors 22 (9) (2022) 3367, Publisher: MDPI.
[162] Y. Zhang, J. Xu, Z. Wang, R. Geng, K.-K.R. Choo, J.A. Pérez-Díaz, D. Zhu, Efficient and intelligent attack detection in software defined iot networks, in: 2020 IEEE International Conference on Embedded Software and Systems, ICESS, IEEE, 2020, pp. 1–9.
[163] Z.U.A. Tariq, E. Baccour, A. Erbad, M. Guizani, M. Hamdi, Network intrusion detection for smart infrastructure using multi-armed bandit based reinforcement learning in adversarial environment, in: 2022 International Conference on Cyber Warfare and Security, ICCWS, IEEE, 2022, pp. 75–82.
[164] S. Khare, M. Totaro, Ensemble learning for detecting attacks and anomalies in iot smart home, in: 2020 3rd International Conference on Data Intelligence and Security, ICDIS, IEEE, 2020, pp. 56–63.
[165] K. Nimmy, M. Dilraj, S. Sankaran, K. Achuthan, Leveraging power consumption for anomaly detection on IoT devices in smart homes, J. Ambient Intell. Humaniz. Comput. (2022) 1–12, Publisher: Springer.
[166] F. Alghayadh, D. Debnath, HID-SMART: Hybrid intrusion detection model for smart home, in: 2020 10th Annual Computing and Communication Workshop and Conference, CCWC, 2020, pp. 0384–0389, http://dx.doi.org/10.1109/CCWC47524.2020.9031177.
[167] Y. Meidan, D. Avraham, H. Libhaber, A. Shabtai, CADeSH: Collaborative anomaly detection for smart homes, IEEE Internet Things J. (2022) Publisher: IEEE.
[168] M. Hegde, G. Kepnang, M. Al Mazroei, J.S. Chavis, L. Watkins, Identification of botnet activity in IoT network traffic using machine learning, in: 2020 International Conference on Intelligent Data Science Technologies and Applications, IDSTA, 2020, pp. 21–27, http://dx.doi.org/10.1109/IDSTA50958.2020.9264143.
[169] X. Dai, J. Mao, J. Li, Q. Lin, J. Liu, HomeGuardian: Detecting anomaly events in smart home systems, Wirel. Commun. Mob. Comput. 2022 (2022) Publisher: Hindawi.
[170] D. Yuan, K. Ota, M. Dong, X. Zhu, T. Wu, L. Zhang, J. Ma, Intrusion detection for smart home security based on data augmentation with edge computing, in: ICC 2020 - 2020 IEEE International Conference on Communications, ICC, 2020, pp. 1–6, http://dx.doi.org/10.1109/ICC40277.2020.9148632, ISSN: 1938-1883.
[171] T.V. Ramana, M. Thirunavukkarasan, A.S. Mohammed, G.G. Devarajan, S.M. Nagarajan, Ambient intelligence approach: Internet of Things based decision performance analysis for intrusion detection, Comput. Commun. 195 (2022) 315–322, Publisher: Elsevier.
[172] Y. Wan, K. Xu, G. Xue, F. Wang, IoTargos: A multi-layer security monitoring system for Internet-of-Things in smart homes, in: IEEE INFOCOM 2020 - IEEE Conference on Computer Communications, 2020, pp. 874–883, http://dx.doi.org/10.1109/INFOCOM41043.2020.9155424, ISSN: 2641-9874.
[173] A.K. Shukla, S. Dwivedi, Discovery of Botnet activities in Internet-of-Things system using dynamic evolutionary mechanism, New Gener. Comput. 40 (1) (2022) 255–283, Publisher: Springer.
[174] N.K. Sahu, I. Mukherjee, Machine learning based anomaly detection for IoT network: (Anomaly detection in IoT network), in: 2020 4th International Conference on Trends in Electronics and Informatics, ICOEI 48184, 2020, pp. 787–794, http://dx.doi.org/10.1109/ICOEI48184.2020.9142921.
[175] X. Li, H. Ghodosi, C. Chen, M. Sankupellay, I. Lee, Improving network-based anomaly detection in smart home environment, Sensors 22 (15) (2022) 5626, Publisher: MDPI.
[176] T. Li, Z. Hong, L. Yu, Machine learning-based intrusion detection for IoT devices in smart home, in: 2020 IEEE 16th International Conference on Control Automation, ICCA, 2020, pp. 277–282, http://dx.doi.org/10.1109/ICCA51439.2020.9264406, ISSN: 1948-3457.

[177] N. Butt, A. Shahid, K.N. Qureshi, S. Haider, A.O. Ibrahim, F. Binzagr, N. Arshad, Intelligent deep learning for anomaly-based intrusion detection in IoT smart home networks, Mathematics 10 (23) (2022) 4598, Publisher: MDPI.
[178] O. Toutsop, P. Harvey, K. Kornegay, Monitoring and detection time optimization of man in the middle attacks using machine learning, in: 2020 IEEE Applied Imagery Pattern Recognition Workshop, AIPR, 2020, pp. 1–7, http://dx.doi.org/10.1109/AIPR50011.2020.9425304, ISSN: 2332-5615.
[179] N. Dat-Thinh, H. Xuan-Ninh, L. Kim-Hung, MidSiot: A multistage intrusion detection system for Internet of Things, Wirel. Commun. Mob. Comput. 2022 (2022) Publisher: Hindawi.
[180] R. Gassais, N. Ezzati-Jivan, J.M. Fernandez, D. Aloise, M.R. Dagenais, Multi-level host-based intrusion detection system for Internet of Things, J. Cloud Comput. 9 (1) (2020) 62, http://dx.doi.org/10.1186/s13677-020-00206-6.
[181] P. Anand, Y. Singh, H. Singh, M.D. Alshehri, S. Tanwar, SALT: Transfer learning-based threat model for attack detection in smart home, Sci. Rep. 12 (1) (2022) 12247, Publisher: Nature Publishing Group UK London.
[182] M. Eskandari, Z.H. Janjua, M. Vecchio, F. Antonelli, Passban IDS: An intelligent anomaly-based intrusion detection system for IoT edge devices, IEEE Internet Things J. 7 (8) (2020) 6882–6897, http://dx.doi.org/10.1109/JIOT.2020.2970501, Conference Name: IEEE Internet of Things Journal.
[183] W.A. Alonazi, H. Hamdi, N.A. Azim, A.A.A. El-Aziz, SDN architecture for smart homes security with machine learning and deep learning, Int. J. Adv. Comput. Sci. Appl. (IJACSA) 13 (10) (2022) http://dx.doi.org/10.14569/IJACSA.2022.01310108, Number: 10 Publisher: The Science and Information (SAI) Organization Limited URL https://thesai.org/Publications/ViewPaper?Volume=13&Issue=10&Code=IJACSA&SerialNo=108.
[184] F. Alghayadh, D. Debnath, Performance evaluation of machine learning for prediction of network traffic in a smart home, in: 2020 11th IEEE Annual Ubiquitous Computing, Electronics Mobile Communication Conference, UEMCON, 2020, pp. 0837–0842, http://dx.doi.org/10.1109/UEMCON51285.2020.9298134.
[185] B.B. Gupta, P. Chaudhary, X. Chang, N. Nedjah, Smart defense against distributed denial of service attack in IoT networks using supervised learning classifiers, Comput. Electr. Eng. 98 (2022) 107726, Publisher: Elsevier.
[186] M. Usman, V. Muthukkumarasamy, X. Wu, Mobile agent-based cross-layer anomaly detection in smart home sensor networks using fuzzy logic, IEEE Trans. Consum. Electron. 61 (2) (2015) 197–205, http://dx.doi.org/10.1109/TCE.2015.7150594.
[187] M. Gajewski, J.M. Batalla, G. Mastorakis, C.X. Mavromoustakis, A distributed IDS architecture model for smart home systems, Clust. Comput. the J. Netw. Softw. Tools Appl. 22 (2019) 1739–1749, http://dx.doi.org/10.1007/s10586-017-1105-z.
[188] J. Liu, J. He, W. Zhang, T. Ma, Z. Tang, J.P. Niyoyita, W. Gui, ANID-SEoKELM: Adaptive network intrusion detection based on selective ensemble of kernel ELMs with random features, Knowl.-Based Syst. 177 (2019) 104–116, http://dx.doi.org/10.1016/j.knosys.2019.04.008, URL https://www.sciencedirect.com/science/article/pii/S095070511930173X.
[189] G. Pinto, Z. Wang, A. Roy, T. Hong, A. Capozzoli, Transfer learning for smart buildings: A critical review of algorithms, applications, and future perspectives, Adv. Appl. Energy 5 (2022) 100084, http://dx.doi.org/10.1016/j.adapen.2022.100084, URL https://www.sciencedirect.com/science/article/pii/S2666792422000026.
[190] NSL-KDD, URL https://www.unb.ca/cic/datasets/nsl.html.
[191] CASAS smart home data sets, 2009, URL http://casas.wsu.edu/datasets/.
[192] N. Moustafa, J. Slay, UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set), in: 2015 Military Communications and Information Systems Conference, MilCIS, 2015, pp. 1–6, http://dx.doi.org/10.1109/MilCIS.2015.7348942.
[193] Y.M.P. Pa, S. Suzuki, K. Yoshioka, T. Matsumoto, T. Kasama, C. Rossow, IoTPOT: Analysing the rise of IoT compromises, in: 9th USENIX Workshop on Offensive Technologies, WOOT 15, 2015.
[194] SherLock Dataset, URL https://www.kaggle.com/BGU-CSRC/sherlock.
[195] CSE-CIC-IDS2018, URL https://www.unb.ca/cic/datasets/ids-2018.html.
[196] DS2OS traffic traces, URL https://www.kaggle.com/francoisxa/ds2ostraffictraces.
[197] N. Koroniotis, N. Moustafa, E. Sitnikova, B. Turnbull, Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset, Future Gener. Comput. Syst. 100 (2019) 779–796, http://dx.doi.org/10.1016/j.future.2019.05.041, URL https://www.sciencedirect.com/science/article/pii/S0167739X18327687.
[198] H.K. Kim, IoT network intrusion dataset, 2019, Publisher: IEEE Type: dataset URL https://ieee-dataport.org/open-access/iot-network-intrusion-dataset.
[199] A. Sivanathan, H.H. Gharakheili, F. Loi, A. Radford, C. Wijenayake, A. Vishwanath, V. Sivaraman, Classifying IoT devices in smart environments using network traffic characteristics, IEEE Trans. Mob. Comput. 18 (8) (2019) 1745–1759, http://dx.doi.org/10.1109/TMC.2018.2866249, Conference Name: IEEE Transactions on Mobile Computing.
[200] I. Ullah, Q.H. Mahmoud, A scheme for generating a dataset for anomalous activity detection in IoT networks, in: C. Goutte, X. Zhu (Eds.), Advances in Artificial Intelligence, in: Lecture Notes in Computer Science, Springer International Publishing, Cham, 2020, pp. 508–520, http://dx.doi.org/10.1007/978-3-030-47358-7_52.
[201] IoT-23: A labeled dataset with malicious and benign IoT network traffic | Zenodo, URL https://zenodo.org/record/4743746.
[202] Papers with Code - Machine Learning Based IoT Intrusion Detection System: An MQTT Case Study (MQTT-IoT-IDS2020 Dataset), URL https://cs.paperswithcode.com/paper/machine-learning-based-iot-intrusion.
[203] N. Moustafa, A new distributed architecture for evaluating AI-based security systems at the edge: Network TON_IoT datasets, Sustainable Cities Soc. 72 (2021) 102994, http://dx.doi.org/10.1016/j.scs.2021.102994, URL https://www.sciencedirect.com/science/article/pii/S2210670721002808.
[204] General Data Protection Regulation (GDPR) – Official Legal Text, URL https://gdpr-info.eu/, Publication Title: General Data Protection Regulation (GDPR).
[205] Y. Luo, L. Yin, W. Bai, K. Mao, An appraisal of incremental learning methods, Entropy 22 (11) (2020) 1190, http://dx.doi.org/10.3390/e22111190, URL https://www.mdpi.com/1099-4300/22/11/1190.