# Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey

Edward Staddon, Valeria Loscri, Nathalie Mitton

applied sciences

MDPI

*Review*

# Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey

**Edward Staddon *, Valeria Loscri and Nathalie Mitton**

Inria Lille-Nord Europe/FUN, 59650 Villeneuve-d'Ascq, France; valeria.loscri@inria.fr (V.L.); nathalie.mitton@inria.Fr (N.M.)
* Correspondence: edward.staddon@inria.fr

**Abstract:** With the ever advancing expansion of the Internet of Things (IoT) into our everyday lives, the number of attack possibilities increases. Furthermore, with the incorporation of the IoT into Critical Infrastructure (CI) hardware and applications, the protection of not only the systems but the citizens themselves has become paramount. To do so, specialists must be able to gain a foothold in the ongoing cyber attack war-zone. By organising the various attacks against their systems, these specialists can not only gain a quick overview of what they might expect but also gain knowledge into the specifications of the attacks based on the categorisation method used. This paper presents a glimpse into the area of IoT Critical Infrastructure security as well as an overview and analysis of attack categorisation methodologies in the context of wireless IoT-based Critical Infrastructure applications. We believe this can be a guide to aid further researchers in their choice of adapted categorisation approaches. Indeed, adapting appropriated categorisation leads to a quicker attack detection, identification, and recovery. It is, thus, paramount to have a clear vision of the threat landscapes of a specific system.

**Keywords:** cyber attack; attack categorisation; cyber security; IoT; critical infrastructures; challenges; data sets



**Citation:** Staddon, E.; Loscri, V.; Mitton, N. Attack Categorisation for IoT Applications in Critical Infrastructures, a Survey. *Appl. Sci.* **2021**, *11*, 7228. https://doi.org/10.3390/app11167228

Academic Editors: Marc Kurz and Erik Sonnleitner

Received: 28 June 2021
Accepted: 26 July 2021
Published: 5 August 2021



## 1. Introduction

The National Institution of Standards and Technology (NIST) (https://www.nist.gov/ accessed on 2 August 2021) defines a cyber attack as a cyberspace attack targeting a business cyber system with varying degrees of malicious consequences, such as disrupting infrastructure functionality or data destruction [1]. With increasing numbers of advances being made every day towards the sector of Information Technology (IT), attackers must adapt to stay on top. To do so, they must evolve their existing attack methodologies, thus, creating newer and improved attacks to fulfil their objectives.

Coincidentally, cyber security specialists must also stay on their toes to be able to secure these new IT systems from an attack, whilst also taking into account new threats that will inevitably be developed. This vicious circle represents the ongoing battle in cyber security to protect and secure before an attack can take place. Unfortunately, even with these proactive methods, it is not always possible to fully secure against all threats, which, in many cases, can cause devastating consequences depending on the system compromised. Furthermore, these technological advancements also create new entry points for attackers to exploit, thus, adding to the already significant task of system protection.

In this paper, we focus on the different methods of categorisation employed in the literature. Furthermore, we explore these methods from within the context of the Internet of Things (IoT), in particular IoT-based wireless devices in the area of Critical Infrastructures (CI), undertaken as part of the CyberSANE https://www.cybersane-project.eu/ accessed on 2 August 2021 H2020 project.

We provide a novel insight and understanding of attack categorisation through the analysis of the different methodologies used throughout the scientific community. Indeed,

due to the vast quantity and diversity of cyber attacks in the cyberspace, specialists must be capable of organising threats to their systems in an easy and understandable way. Such categorisation techniques, therefore, provide the capacity to structure and organise the various attacks, based upon the specifications of the underlying system.

We undertake this study from the initial standing point of a bystander, basing our analysis upon the categories themselves as explained in the literature. We then conclude our study by shifting our point of view to that of CI IoT wireless applications. From the stand point of CI systems and their IoT applications, we gain an insight into the different characteristics and security challenges encountered with these systems. Critical Infrastructures bring new constraints, mainly in terms of time responses, recovering delays, and data protection, especially when focusing on wireless systems, which are more prone to attacks due to their pervasive nature.

*Structure*

We start with a presentation of the context in which this survey is undertaken by defining our background situation in Section 2. In Section 3, we provide a preliminary discussion regarding the notion of cyber attacks as well as the need for categorisation approaches before presenting the various methodologies in Section 4. In Section 5, we provide an overview and in-depth analysis of the categorisation methods from Section 4 before discussing some of the various challenges encountered in cyber security as well as an overview of available data sets in Section 6. We conclude with a discussion about the lessons learnt during the construction of this survey in Section 7 before concluding the survey in Section 8.

## 2. Background

In this section, we develop and present the context in which this survey is undertaken. As defined previously, we orient our analysis from the standing point of IoT wireless devices in Critical Infrastructures. First, we present and define the notion of Critical Infrastructures, before moving onto the specificities of wireless communications. Finally, we define the notion of the Internet-of-Things and the unique qualities of such devices.

### *2.1. Critical Infrastructures*

When a cyber system is compromised, the goal could be of different natures. One of the most common is to access private and secure information and rendering it public or selling it to the highest bidder, such as the attack against a South Korean company in December 2014 [2]. In this attack, hackers compromised a South Korean nuclear and hydroelectric company, stealing technical data concerning their two nuclear reactors, as well as the personal data of 10,000 employees.

A second nature is to impact the operation of the target, rendering it unusable and consequently causing disruption to its operational control, such as the Saudi Arabia petrochemical plant attack in August 2018 [3]. During this attack, the petrochemical plant was sabotaged causing it to shutdown; however, specialists believe that the intention was instead to cause significant damage by sabotaging the safety operations in order to cause an explosion.

Any of these attacks are critical when targeting important infrastructures that are vital to the operations of a nation. These Critical Infrastructures (CIs) cover multiple sectors [4], such as healthcare, transport, energy, and financ, as well as government systems, which, as a consequence, are often the target for cyber attacks. Unfortunately, the critical nature of these systems means that, in many cases, an attack can cause significant disruption to the internal workings of a nation and, in certain cases, even cause the death of civilians.

With the many technological leaps being made, more CI dependant technologies are being deployed amongst the civilian population. For example, small healthcare devices belonging to a hospital, such as connected heart-rate sensors, share data with medical personnel, allowing them to react to changes in the patients body chemistry. As such,

these devices belong to this CI and being in the possession of a civilian, increase the risk towards them if the device were to become compromised. As a consequence, CI protection is paramount and part of many ongoing cyber security research projects [5].

### 2.2. Wireless Communications

Securing CIs is an important task, even more so with the evolution and incorporation of wireless communications into increasing devices and equipment on a larger scale and the inclusion of IoT. The IoT requires new methods for attack categorizations compared to Wireless Sensor Networks (WSN) and Mobile Ad-hoc NETworks (MANET) since these objects are known as very weak. They are limited in computing capacities, which prevents them from embedding very secured code and relied on limited power sources prone to attacks leading to an energy drains and a stop of the service these IoT devices are expected to deliver.

With this addition, these devices can join the plethora of other types of CI equipment that are interconnected with each other through the Internet However, although network access grants the possibility for attackers to access previously inaccessible targets, the use of the wireless medium also provides other issues. Although many different wireless protocols exist for various types of uses, the most common and even mainstream technologies, such as Wi-Fi and Bluetooth, all use the same portion of the radio spectrum, reserved internationally for Industrial, Scientific, and Medical (ISM) purposes.

Since the ISM band is free access, it is, therefore, shared with a multitude of different devices, from home network devices to microwaves. As such, all data transiting through this public domain is susceptible of being captured, analysed, or even exploited. Furthermore, unlike wired networks where direct access to the infrastructure is required, attacks can exploit the wireless radio range to interact with the target network.

Protecting and securing wireless communications is an ongoing challenge, since the medium is both shared and inherently unprotected. Many solutions exist to protect the exchange of data, such as the common security protocols Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access II (WPA2). However, these systems are not infallible and, when broken, lose their usefulness.

This is even more significant when noting the widespread use of WPA2, which, after 14 years of certification, was broken in 2017 [6]. In many cases, these protocols are not used as their many uses are towards Infrastructure-centric networks, revolving around a single network access point. In point-to-point ad-hoc networks, however, each device establishes its own links with its neighbours. This means that each participant must be capable of securing all communications between themselves and the interlocutor. Securing these exchanges, as well as rendering the everyday wireless network usage more robust is also an ongoing challenge.

### 2.3. Internet of Things (IoT)

With the increase in available possibilities for intercommunication, increasing devices are joining the digital world. From small gadgets to home appliances, the upsurge of such "things" becoming interconnected forms a new networking and operational paradigm. This Internet of Things (IoT) allows many areas, such as agriculture and healthcare as well as the military to expand their numerical workforce with autonomous devices, such as remote weather stations, connected pacemakers, and even remote battlefield sensors. These intelligent devices help increase the quality of life by contributing towards these areas through information sharing.

However, due to their various areas of application, such devices posses certain limitations and constraints on both a hardware and an application level. For example, in remote deployment scenarios, energy is a rare commodity and, therefore, must rely on battery packs. However, the various operational necessities of such devices, in particular wireless communications, are, in general, power hungry. Thus, these limited energy

reserves impose further limitations on device hardware, such as decreasing computational capabilities as well as limiting communication possibilities.

### 2.4. Categorisation

With the increasing number of attacks targeting the various systems and technologies previously mentioned, the subject of cyber security has become of increasing interest in the scientific community. Indeed, more researchers are participating in the ongoing battle with attackers to provide solutions to secure various systems and protocols. However, to be able to provide solutions to these problems, the existing threats must first be defined and evaluated.

To do so, attacks are organised into different categories depending on specific criteria. Furthermore, with the large interest in cyber security comes multiple publications in the literature, each presenting and exploring various threats in cyber space. In doing so, they use a categorical structure to organise their workflow and label the various attacks studied.

Unfortunately, the choice of categories is generally up to the author, meaning that many different approaches exist, sometimes intermixing from paper to paper. In some cases, multiple approaches are fused into one large structure, providing a varying degree of specification and organisation. In short, when analysing threats against multiple systems, such as present in CIs, many different methods can be used. Also, since many attacks can be performed whatever the network medium employed (wireless or wired), and can impact both IoT and industrial hardware alike, understanding the different stand points of each categorical approach is a significant advantage.

## 3. Preliminary Discussion

In this section, we will begin by discussing the notion of cyber attacks in general, presenting how they are achieved and the various steps undertaken by an attacker during an attack. Following on, we will present the different Security Principles in pace in IoT networks before finally, following up with a brief overview of why categorisation techniques are needed to analyse and structure these attacks.

### 3.1. Cyber Attacks

A "kill chain" (originally used as a military concept related to the structure of an attack) consists of target identification, force dispatch to the target, a decision and order to attack the target, and finally the destruction of the target. Although this term acceptance is not universal, the cyber kill chain model has seen some adoption in the information security community. This section describes the different steps in a cyber kill chain and how they can be explored to identify, detect, and counter balance a cyber attack.

As stated previously, the notion of "cyber attacks" is generally used to present an aggressive act towards a computer or electronic device. However, the term represents much more that the attack itself. In [7], it is mentioned that cyber attacks is a grouping of multiple stages, such as the notion of reconnaissance or Denial-of-Service. However, they go into more detail explaining that the notion of cyber attacks consists of five distinct steps, each with their own independent objectives towards the successful completion of an attack in the cyber-space.

Since these five stages are critical to the success of a cyber attack, any defensive barrier erected against any stage will cause a disruption in the attackers efforts and increase the overall difficulty. With the constant development of malicious platforms and methodologies to perform attacks, their reach in terms of targeting systems with increasing IoT devices residing in the cross-hairs is becoming limitless. However, one constant across all systems, whether IoT-based or employing specific network protocols, are the five attack steps that remain generally the same.

Although the overall methodologies remain constant, certain particularities are inevitable due to various device or network limitations. For example, IoT devices may see certain

types of logs omitted due to hardware constraints imposing strict limitations upon storage space. The five categories are presented in Figure 1, and we detail them below.

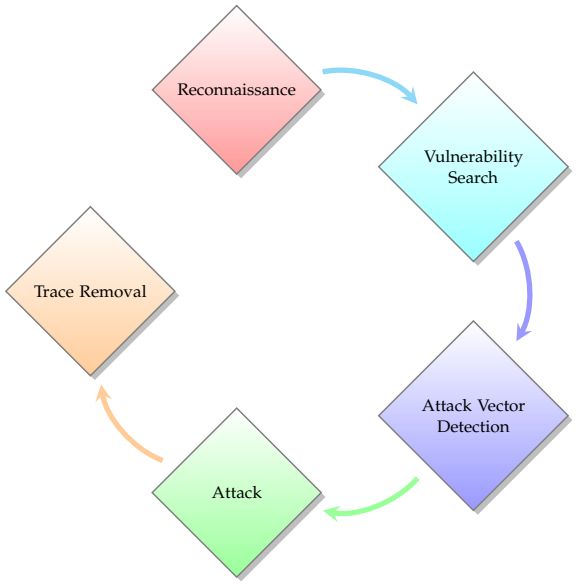


**Figure 1.** Cyber Attack Steps.

#### 3.1.1. Reconnaissance

Similar to its military cousin, reconnaissance is the act of gathering information [8], covertly or not. If we assimilate a cyber-space attack to a covert war zone equivalent, this becomes more apparent. Soldiers will aim to discover the layout of the target environment, as well as the different infrastructures and vehicles possessed by the enemy to gain the upper hand during combat. They also scout out critical targets, which, when attacked, could cause a significant disruption to enemy operations.

Back in cyber-space, these targets possess numerical equivalents, such as the discovery of the network topology, as well as the different software solutions and Operating Systems used or even the type of device itself. Lastly, critical targets hold the same importance towards the target system as they do to an enemy army on the battlefield. In [9], some examples of information gathered are presented, including IP addresses and user names as well as firewall systems and, more significantly, even home addresses and telephone numbers.

#### 3.1.2. Vulnerability Search

The recovered information is in itself useless without proper analysis. Performing an in-depth examination can provide significant information that the attacker can exploit, giving them the upper hand. The evaluation allows the discovery of existent weaknesses in the different systems, such as long grass allowing covert advancements on the battlefield, an unlocked door at the enemy HQ, and low fuel reserves.

For cyber-systems, these items concern vulnerabilities in the Software used, the OS, or even Network or hardware weak points [10]. Exploiting such vulnerabilities can make the attackers job easier due to their susceptibility to certain types of attacks. As such, due to the somewhat limited choices between security systems in certain infrastructures, a successful aggression against one system is potentially possible against another. This was illustrated by the cyber attack against the Ukrainian power grid where vulnerabilities could be present in other power systems world wide [11].

#### 3.1.3. Attack Vector Detection

Possessing a list of weaknesses, it is possible to determine the best means of attack. As such, the attacker's objective is the identification and extrapolation of an entry point, allowing them access to the target area. In a military scenario, soldiers will look for covered

areas to hide their approach in the different defences both in the surrounding area and in the immediate vicinity of the target.

With the internet now reaching every home and practically every electronic device, network attacks are the most common occurrence. The attacker, therefore, from the previously obtained list of network and system vulnerabilities, examines the network layout as well as the defensive measures in place. However, this only grants the attacker access to the network; thus, an analysis of the system defences of the target is also necessary From this, the attacker can choose from a multitude of vectors dependant on each vulnerability, as explained in [12].

#### 3.1.4. Attack

With the arsenal of knowledge now at the attacker's disposal, it is now possible to begin the assault. There is no fixed unique methodology to undertake such an attack, since the desired outcome as well as the system specifications vary. The previously recovered information, however, allows the attacker to determine the best possible methods to inflict the desired consequences.

#### 3.1.5. Trace Removal

Once the objective is complete, the attackers can simply exit the target system, knowing that they have accomplished what they set out to do. However, operations on computer systems leave traces, which can be used by cyber security specialists to piece together the attack and even perform a backtrace, eventually identifying the attacker.

Once again, in the same manner as an undercover military operation, once the objective is accomplished, the soldiers must be extracted without discovery. This means covering certain tracks and preventing the enemy from identifying the orchestrator of the attack.

With cyber-systems, this can be accomplished through either Log purging or manipulation. The former is the simplest, but leaves behind a blank log file, which, on a running system, is extremely suspicious. The second is thus the most advantageous although the most difficult, since manipulating the log file removes all traces of the attack, whilst leaving the normal logged operations behind. This method not only removes the ability of knowing what happened on the system; however, it also reduces the risk of immediate detection.

As stated previously, certain devices, such as IoT hardware constrained devices, posses certain limitations upon their operation. An example is the limitations imposed upon the type of storage media used, thus, impacting the available space. Since certain IoT devices are meant to be left alone to their own accord for long periods of time without administrative access, certain restrictions are imposed upon their functionality to preserve operations at all costs. One sacrifice, for instance on a remote sensor deployed in a hostile environment, is that log files are not needed when retrieving the device is not an option. As such, this final attack step can not be necessary, or even possible.

### *3.2. IoT Security Principles*

To be able to grasp our viewpoint of IoT security in CIs, an understanding of their specific security needs is important. Since IoT devices are becoming increasingly present in our lives, we start to rely on them to help make certain menial tasks easier. Unfortunately, they not only usher in a new technical age, but also a new area in which cyber-criminals can thrive. IoT security is an ever developing area due to the unique nature of certain devices. To aid in the development of security systems and protection methods for IoT devices and networks, multiple security concerns have been determined.

Many of these security principles presented in Figure 2, such as Confidentiality, Integrity, Availability, and Authentication [13], are not specific to IoT applications and are shared with cyber systems in general. However, specific security features revolve around the different characteristics of IoT devices and networks as presented in [14].

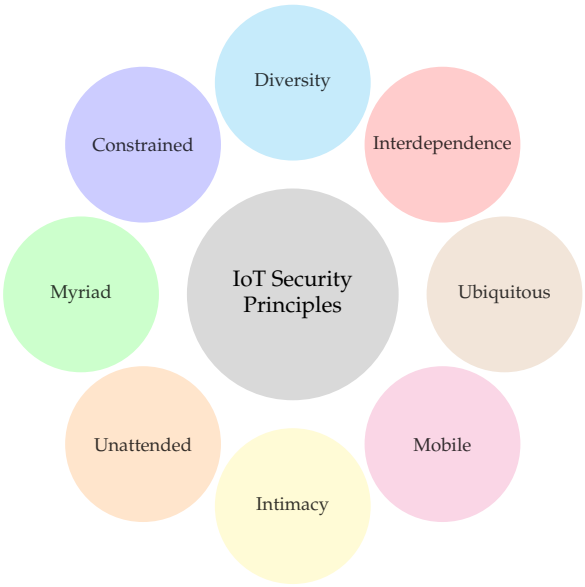


**Figure 2.** IoT Security Principles.

#### 3.2.1. Interdependence

With the development of self-contained autonomous devices, the need for human interaction is decreasing. Indeed, such smart devices are capable of making decisions based upon various factors, such as the environment or other devices themselves. This function is the basis for both Smart Home applications and Industrial systems that use cloud-based rules to define actions based upon sensory input. An example of the former would be the activation of smart bulbs when the indoor light level in a room drops below a certain threshold. In certain cases, this chain of events can be taken advantage of by interacting with a single device, such as a sensor, which, in turn, can activate another device.

In the previous example, an attacker can trick a sensor into thinking the light level is higher than in reality, which will deactivate the bulbs in the vicinity, plunging the room into darkness, making it easier to penetrate into the accommodation undetected.

#### 3.2.2. Diversity

In the aforementioned Smart Home scenario, multiple devices must coexist in harmony, such as smart bulbs, plugs, switches, and multiple types of sensors. Each of these devices was constructed to perform a certain task and, as such, possesses specific hardware to that effect. Furthermore, these devices must communicate amongst themselves, and, in many cases, multiple devices in the same environment use different protocols, such as Zigbee or Bluetooth. These diversity is an inherent feature of IoT networks, but also introduces security risks due to the different devices that need protecting.

#### 3.2.3. Constrained

As mentioned previously, IoT devices posses certain hardware limitations. In many cases, some devices must be both small and lightweight for certain use cases, such as wearable healthcare devices. As such, their limited dimensions impose certain hardware construction limitations, reducing the storage capacity, energy reserves, computation capabilities, as well as communication technologies.

These limitations are naturally adapted towards the specific environment in which the device is to be used. For example, in the previous healthcare example, a connected pacemaker needs to capture and transmit data in real-time, putting importance on data acquisition and communication. However, in a military application, energy consumption is significantly more important due to the somewhat remote deployment measures sometimes undertaken.

#### 3.2.4. Myriad

With the previous limitations imposed on certain devices, it is easier to create and deploy. This increase of devices leads to more interconnections between devices, increasing the network complexity. Furthermore, the more devices that are deployed in an IoT network, the higher the risk of a device being compromised due to the large diversity of devices leading to the increasing chance of the apparition of network or device vulnerabilities. This was referred to as Myriad by the authors of [14].

#### 3.2.5. Unattended

In certain areas, such as agriculture or military, devices are occasionally deployed in remote areas. This reduces the possibility of human interaction or supervision and even, in some cases, renders them impossible. This means these devices must become fully autonomous and also be capable of communicating amongst themselves. Thus, wireless networking technologies are favoured allowing communication over various distances dependant on the technology employed, facilitating the deployment itself.

#### 3.2.6. Intimacy

Due to the increased usage of IoT devices in our day-to-day lives, the question of privacy is naturally present. Since many devices are constantly capturing data, such as a Smart Watch capturing a person's heart rate or a GPS chip capturing the location of the device, the way the information is shared and analysed must be taken into account.

In this paper, we will not go into detail regarding the notions of Privacy but will interest ourselves more towards attacks and security measures.

#### 3.2.7. Mobile

Another particularity of IoT devices is the ability to be deployed in a mobile environment, such as on a city bus service or a wearable smart device. Unlike in static applications, the environment in which these devices reside is constantly evolving, impacting their communication capabilities. For a device to remain connected, it must be capable of jumping from one network to another. This hopping results in the device joining a new unknown network, where it can communicate with previously unknown devices. For example, Smart Buses move around the city jumping from network to network allowing them to update the expected arrival time at the next bus stop.

#### 3.2.8. Ubiquitous

Increasing amounts of people rely on IoT devices as part of their lives, making them become an integral part of their being. The authors of [14] referred to this phenomenon as the "ubiquitous" nature. This increases the risk of security-related incidents, not from a hardware point of view but, instead, from human interaction. Indeed, the phrase "the error is generally found between the chair and the keyboard" when concerning IT issues is generally true since human error is a large contributing factor. As such, threats can be perceived from multiple angles, from the manufacturer to the private or professional consumers and operators but also the security research experts.

### *3.3. Need for Categorisation*

As stated previously, the fourth stage of cyber attacks consists of performing various attacks upon a target system. However, since there are multiple types, methodologies, and consequences of cyber attacks, possessing a means to categorise them is a significant advantage.

The use of such a categorisation grants the ability to enumerate the different attacks dependant on a specific common criteria. From this, it is made possible to analyse attackers' strategies and design new adapted and dynamic counter actions to either identify in advance any system vulnerability and fix it or quickly detect an attack and recover. It is, therefore, possible to identify these attacks based on the criteria, making it easier to find a specific attack. However, since there are multiple types of criteria that can be used for

categorisation, the choice is dependant on the intended use, but also on the types of attacks; for example, network-based attacks will not be categorised the same way as physical access to a device.

## 4. Attack Categorisation

As stated previously, attack categorisation is an important factor when dealing with cyber attacks due to the large numbers of attack methodologies. However, with these numbers also comes the risk of multiple categorisation methods, each with their own advantages. In this section, we will explore some categorisation techniques, as well as the different approaches in use in the literature. Overall, we have documented eight distinct categorical methodologies, each with different approaches in structuring their attacks. Table 1 presents an overview of these possible categorisation approaches.

**Table 1.** Compilation of attack categorisation approaches.

| Categorisation | Description |
|---|---|
| Attack Severity | Organised dependant on the severity of the attack or the threat level |
| Access Type | Organised dependant upon the type of access used by the attack |
| Attack Type | Organised dependant on the type overall type of attack |
| Attacker Position | Organised dependant on the attackers position relative to the victim |
| Attacker Implication | Organised dependant on the interaction between attacker and victim |
| Objective Oriented | Organised dependant on the overall goal of the specific attack |
| Network Layer Oriented | Organised dependant on the OSI layer where the attack resides |
| Use-Case Specific | Organised dependant on the specific use case |

### *4.1. Attack Severity*

Likely the most basic categorisation method used in cyber security is the separation based upon the severity of the attack. In [15], the UK National Cyber Security Centre proposed an attack categorisation based on six threat levels, from the lowest being a localised incident, to the highest corresponding to a national cyber emergency. This categorisation, however, is not only heavily dependant on both the type of environment and systems available but also severely influenced by the organism designing such a proposition, as, with dependence on the environment, various attacks will cause more or less disruption.

### *4.2. Access Type*

Another most basic form of attack categorisation is the separation based upon the type of access exploited. In this case, the type of access is defined as the basic interaction methods used to commit the attack. In [16], the authors define cyber attacks in their taxonomy as pertaining to two categories: Physical and Cyber.

This approach opposes the two extreme global methods of assaulting an IT system. Physical attacks, as their name states define a physical interaction with the IT system, leading to threats, such as tampering, hardware damage, or simply physical access to an administrator interface terminal. An example of a Physical attack is the assault on California Power Station by a Sniper in April 2013 [17]. Cyber attacks on the other hand regroup any threat or assault against these systems from a digital source. This includes attacks from malware installed on the system itself or a remote assault attempt from across the globe through an active network connection.

### *4.3. Attack Type*

Moving forwards, the following form of categorisation evolves around the distinction based upon attack type. Their are many different attack methodologies that exist; however, multiple belong to the same type of attack. An example is the *Denial-of-Service* (*DoS*) attack shown in Figure 3 where the objective is to deny legitimate user access to a shared resource, such as a web server or wireless access point [18].

This can be achieved using various different methods, such as introducing large quantities of data to sensor networks causing data overload, or submerging hardware constrained IoT devices, impacting resources resulting in device shutdown. Furthermore, as presented previously, these devices use wireless communications to exchange with their neighbours. Since the wireless medium is both a shared and rare commodity, monopolising the frequencies can cause long communications blackouts, severely impacting both the operation of the network and the device's resources.

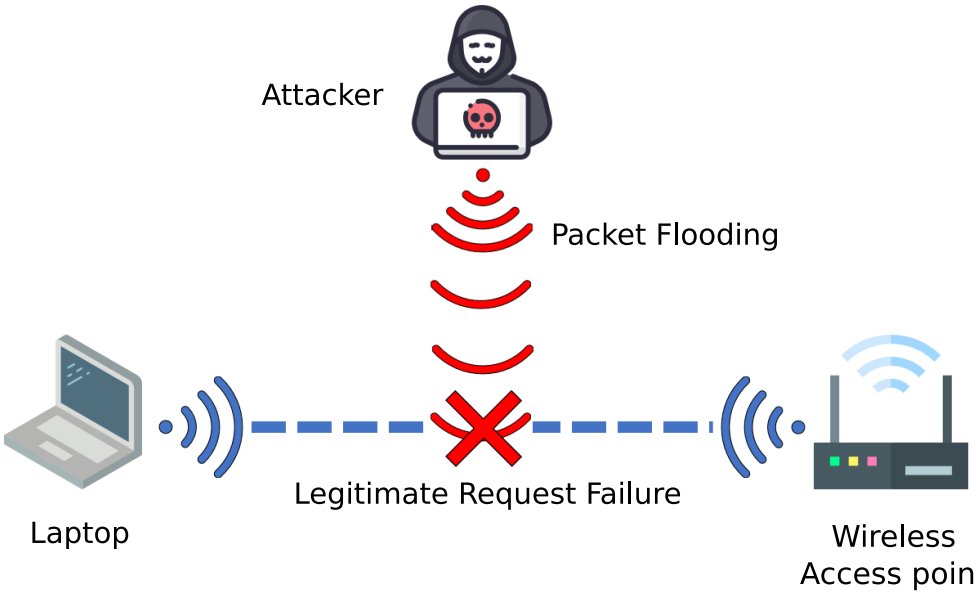


**Figure 3.** Illustration of a Denial-of-Service attack.

A commonly used approach is the differentiation of attacks as being either *DoS*, *Probing*, *Remote-to-Local (R2L)*, or *User-to-Root (U2R)*. As defined in [19], *Probing* attacks are reconnaissance methods to obtain information from a target system, which can then be used for more direct assaults. *R2L* attacks, also known as *Remote-to-User (R2U)*, aim to gain unauthorised access to an IT system from a remote location using obtained user credentials. Following on, a *U2R* attack aims to illegally access an administrative account on the system, from which devastating attacks can be performed.

This approach is used in the presentation of different cyber attack detection strategies in [20], where they present the four different types of cyber attacks that they consider. In [21,22], these four categories are used to define attacks and traffic anomalies for use in attack and anomaly detection systems. This approach can be adapted to various types of networks with their specific limitations and characteristics. For example, in [23], the authors applied this categorisation to deep-learning-based attack detection on IoT-based Fog computing, whereas, in [24], it is used to explain how Brute Force Attacks occur. Furthermore, it is also used in [25] during the analysis of Machine-Learning-based network intrusion detection classifiers.

Following on, another approach is the separation of attacks into three distinct categories: *DoS*, *Man in the Middle (MitM)*, and *Brute Force*. *MitM* is one of the most known attacks in the cyber-space and is illustrated in Figure 4. Studied in [26], this attack places the attacker between two victim devices, forcing traffic to pass through them by tricking each victim to

believe they are communicating with the other. In doing so, the attacker is rewarded access to all exchanges, encrypted or not, meaning it easy to extract information or even modify them to their advantage.

Similar to *DoS* attacks, multiple methodologies exist to perform such an attack, each taking a advantage of a different protocol in the network structure, such as low level ARP-spoofing [27] or high level DNS-poisoning [28]. On the other hand, *Brute Force* attacks, presented in [24], iterate over every possible keystroke in an attempt to find a match and break or decrypt login credentials [29]. Once again, different methods exist for a Brute Force approach, such as a statistical analysis of the most common and recurring characters dependant on the password difficulty. This categorisation is presented in [30] to classify the most common recurring cyber attacks.

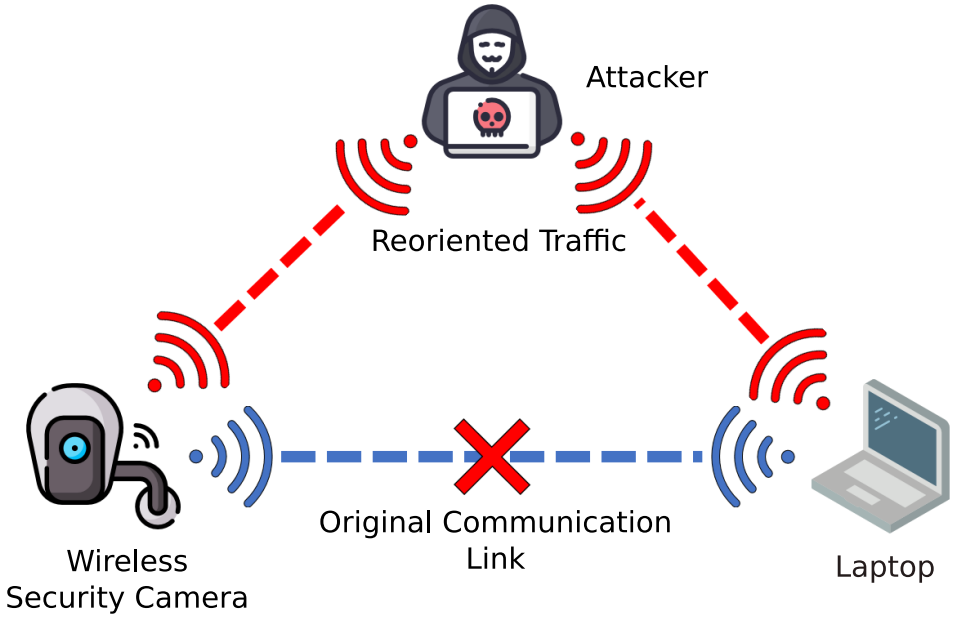


**Figure 4.** Illustration of a Man-in-the-Middle attack.

The use of *DoS* to categorise attacks is quite common. Indeed, it is used in yet another method, separating attacks into three distinct categories: *DoS*, *Replay*, and *Deception*. As explained in [31], *Replay* attacks use legitimate captured data, which is then resent to the original destination. This allows the attacker to gain the trust of the victim, thus, allowing further messages to be sent and accepted by the target. This threat is even more significant in sensitive areas, such as battery-operated IoT medical devices in healthcare [31] where unauthorised access and control of such devices could have significant consequences on the patient's well-being.

*Deception* attacks on the other hand, sometimes called *Integrity attacks* [32] or *False Data-Injection attacks* FDI [33], introduce false data in an attempt to deceive the victim's machine, in turn, forcing it to run invalid operations. Examples of such attacks are against smart grid functionalities, where the introduction of erroneous data into the network seemingly from a legitimate source can alter grid operations, such as altering energy routing [34]. These three categories are used in [35,36] to categorise cyber-threats towards industrial Cyber-Physical Systems (CPSs).

Another classification based on attack type concerns the separation of attacks based upon *Active Eavesdropping*; *Scanning and Probing*; and *Code Injection*. The first category, *Active Eavesdropping*, allows the attacker to increase their spying efficiency by actively interacting with the network, forcing traffic to pass through them [37]. This can be done in many ways, such as *DoS* or *MitM*; for example, it is possible to introduce erroneous data into WSN routing tables, forcing the data to transit via a corrupted node or the attacker themselves [38]. This grants the ability to access and analyse the data, whilst not impacting network operations.

*Scanning and Probing*, on the other hand, although inherently reconnaissance attacks, have as the objective to recover information from a target device. Similar to *Probing* presented above, *Scanning* can recover various types of system or network related information by simply "looking" at what is happening. By looking and evaluating the target environment, it is possible to extract information regarding the devices on the network [39] and even the different vulnerabilities that might exist on these devices [40]. An example of such an attack is the Port Scanning attack, where the goal is to identify and analyse any open and vulnerable ports on a networked device [41].

The final category concerns *Code Injection*, which defines any threat that seeks to introduce malicious code onto a device through unsecured inputs [42]. Such attacks are quite common and generally target applications where inputs are fundamental to their function. For example, many web based application possessing input forms that have not been properly sanitised are rich environments for such injections, as the code is not examined but instead executed by the server [43]. This three-way categorisation is used in [44] to organise multiple stealth attacks against Critical Information Infrastructures.

The final method for categorising attacks based on their type is the use of the following four categories: *Physical*, *Network*, *Software*, and *Encryption*. As defined in the previous section, Physical attacks represent any attack resulting from direct physical access to the device in question. *Network* attacks on the other hand, regroup any attack that is achieved through a network connection, or from a remote source on passing communications. This includes, for example DoS, MitM, the Sybil Attack, and the Sinkhole Attack. The Sybil Attack [45] is defined as the forging of multiple network identities in an attempt to compromise network integrity.

When targeting Wireless Sensor Networks, this attack can cause disruption due to the lack of identity verification between nodes, meaning an unauthorised note with forged identity papers can insert itself into the network. In cases where such networks are in place for monitoring reasons, such as forest wildfire monitoring applications [46], these illicit nodes can counteract legitimate messages and potentially delay a fire response. Sinkhole Attacks on the other hand intervene in the same network paradigm; however, they target directly the routing protocol used [47]. Although devastating to point-to-point communications, this attack is also beneficial and was paramount in stopping the WannaCry ransomware outbreak in 2017 [48].

The third category, *Software*, follows on from this previous example. Indeed, *Software* attacks concern any and all attacks made through malicious programs running on the victim device. This includes threats like Ransomware, which encrypts a victim device and demands a ransom to regain access [49], such as the aforementioned WannaCry [50]; as well as Viruses, a malicious self-replicating program, which infects a target device [51]; or Spyware, malicious code, which snoops and spies on activities and information [52].

The fourth and final category, *Encryption*, allows the organisation of all threats whose objectives are to break encryption systems to recover private keys. These threats include such attacks as Cryptanalysis, which are targeted towards breaking cryptographic protection with no prior knowledge of the encryption method [53]; Side-Channel Attacks, which are the extraction of cryptosystem functions from the analysis of information leakage, for example power consumption or various emissions [54], and even MitM. In [55], this categorisation is used to present the various security attacks possible against IoT networks and devices.

### 4.4. Attacker Position

Another method for categorisation can be achieved based upon the position of the attacker relative to the IT system that is threatened. Such an approach is used in [56] where they utilise the differentiation between Outside and Inside attacks.

As its name states, an *Outside* attack takes place where the origin of the attack is outside of the target infrastructure, such as a remote network attack. This can include threats, such as eavesdropping or DoS attacks. As such, an *Inside* attack is the complete

opposite, where the attacker is already authenticated as part of the infrastructure, such as compromised or malicious devices integrated into the network or simply the exploitation of user authentication.

In [57], they also specify that the attacker position can influence the methods used in various attacks. This approach is also used partly in [13,58,59] to categorise certain attacks pertaining to IoT networks as well as Mobile-Ad-hoc Networks (MANETs) and Software Defined Networks (SDNs), which are explained in more detail in Sections 4.8.3 and 4.8.5.

### 4.5. Attacker Implication

Another common method for attack differentiation is the notion of attacker implication. This approach defines the level of interaction between the attackers themselves and the target system. We discuss, therefore, Active or Passive attacks.

The concept of *Passive* attacks concerns any methodology that does not imply any interaction from the part of the attacker on the target system. This means that the attacker's presence does not influence the outcome of the systems operations, such as an impostor listening behind a closed door. As explained in [20,56], this covers attacks, such as eavesdropping or traffic analysis since the information is recovered through observation or the use of spying software, such as keyloggers. As such, *Passive* attacks are generally considered as being stealthy due to the difficulties in detecting the attacker's activities.

*Active* attacks, however, are the complete opposite of *Passive*, where the attacker is physically invested in the attack itself. In the previous example, the listening impostor opening the door and partaking in the conversation would make him an active participant, thus, influencing the outcome of the system operation. This category includes, for example, data modification, creation, and deletion or simply a DoS attack as presented in [60,61]. This approach is also used in other networking paradigms, such as IoT in [13] and MANETs in [62].

### 4.6. Objective Oriented

A different method for attack categorisation is organisation based on the objective of the specific attack. For example, complementary to their categorisation based on the Access Type presented previously, ref. [16] used the notion of *Privacy*, where they enumerated attacks that recover private information through various spying techniques. These attacks are even more significant depending on the environment in which they reside as the quantity of information varies, for example in an IoT-based smart home, such attacks can recover large quantities of data, encrypted or otherwise for later analysis and exploitation [63].

In [20], the authors complement their already large categorisation methods with the addition of eight independent objective oriented categories: *Reconnaissance*, *Access*, *Malicious*, *Non-Malicious*, *Cyber Crime*, *Cyber Espionage*, *Cyber Terrorism*, and finally *Cyber War*. As presented previously in Section 3.1.1, *Reconnaissance* attacks are the first step towards the realisation of a cyber attack, recovering information concerning the target or its environment. The notion of *Access* attacks on the other hand, as their name states, concern all attacks that attempt to gain unauthorised access to a device. The next two compose two vast categories capable of encompassing all attacks.

Simply put, *Malicious* attacks are deliberate attempts to compromise a system, generally providing an advantage to the attacker, whereas *Non-Malicious* attacks are generally the result of accidental damage or mishandling, causing various degrees of difficulties for system operations. The next four categories concern various degrees of malicious behaviour in the cyber space. The first, *Cyber Crime* covers small attacks where the goal was for the attackers personal gain.

Above this, we can find *Cyber Espionage*, which concerns any spying activities where information recovery is the primary objective. Following on, the next level called *Cyber Terrorism* encompasses any attacks that cause significant damage and disruption to both people and property. Finally, the highest threat level is *Cyber War*, which, in this case,

concerns attacks between nations, where the nation itself is the attacking entity aiming to gain significant advantages over their victim.

Following on from previously, in [44], three more categories complement their three existing attack-type-oriented approaches: *Disconnection and Goodput Reduction*, *Side-Channel Exploitation*, and *Covert-Channel Exploitation*. The first grouping impacts the efficiency of the network connection itself. It, therefore, contains attacks that aim to disconnect devices from the network, stopping them from communication, or by severely impacting and reducing the operational efficiency, called Goodput [64].

Other than impacting network operations, it is possible to use other methods to extract important information regarding internal device operations. In the case of cryptosystems, using *Side-Channel* or *Covert-Channel Exploitation*. Contrary to its *Side-Channel* sibling, which was previously defined, *Covert-Channels* exploit weaknesses in the device configuration where authorised information is shared between two cooperating entities, all the while breaching security policies [65].

In [57], the position of the attacker is mentioned when presenting the various possible attacks. However, they also identify three areas where an attack impact is generally targeted, including an often overlooked aspect: *Hardware*, *Network*, and *Human Factor*. When it comes to Hardware-related attacks, there are many different approaches to significantly impact or exploit the various devices hardware characteristics. For example, Side-Channel attacks as well as malicious software that take advantage of certain device specifications to severely impact or destroy the hardware itself Network attacks, however, cover the many different methods used to impact various different network services by taking advantage if the various characteristics.

For example, attacks against DNS servers, such as DNS-Spoofing or eavesdropping methods, exploit certain characteristics, such as network protocols and the free access to the wireless medium. Finally, the Human Factor covers attacks made by the user, intentionally or not by not adhering to complicated security software or even attacks that target the user themselves, such as Social Engineering, by tricking the user into compromising their system [66]; or Phishing in an attempt to trick the target to provide the attacker with important information, generally through email communications [67].

Previously, the notion of Active or Passive attacker implication was explored, as used in [61]. However, they also extend these two categories, by listing the various attacks therein by pertaining to either *Interception*, *Interruption*, *Fabrication* or *Modification*. These four categories all concern data-related attacks, as their goal is to impact on the efficient sharing of such information. The first category is presented as a subcategory of Passive attacks and concerns the simple *interception* of network messages, breaching confidentiality between the two communicating parties, such as various Scanning activities.

The further three categories are presented as containing Active attacks. *Interruption* attacks cover the different methods as means to stop or impact correct network activities through DoS or an SQL Injection Attack, which takes advantage of unsanitised inputs to access database content [68]. Fabrication and Modification attacks work along the same principal, injecting false data into the network. The main difference between the two is that a Fabrication attack generates its own packets with captured or generated data, such as a Replay Attack, whereas Modification attacks change the values of communications in real time and are generally performed through MitM implementations.

The final categorisation based on the overall objectives, is the separation between attacks impacting *Access Control*, *Authentication*, *Availability*, *Confidentiality*, or *Integrity*. The first set of attacks cover any method used to break or take advantage of existing *Access Control* methods, such as a Rogue Access Point, which will grant an unauthorised back door into a secure system [69]. Following on from *Access Control*, *Authentication* attacks aim to break authentication methods using various methods, such as Brute Force

Next, we can find the various attacks that impact service *Availability*, reducing the capacity for users to use the various services, such as a DoS attack on a web server. Moving on, *Confidentiality* attacks gain to gain access to private communications to extract data,

or example through eavesdropping or a MitM attack. Finally, *Integrity* attacks aim to compromise legitimate data by forging authenticated messages through FDI or Replay attacks. This categorisation is used in [70] to categorise and present various different security threats in wireless networks.

### 4.7. Network Layer Oriented

A method for the categorisation of network-based attacks is the use of the different network layers of the OSI model [71]. This grants the possibility to associate specific attacks to the layer on which their primary impact takes place, such as jamming [72] on the physical layer or a DoS UDP flood [73] on the transport layer.

In practice, attacks are generally categorised on the first four layers as well as the seventh layer. Since the OSI model is the inspiration behind the physical and protocol structure of IP based networks, these five layers can be used to separate the different threats towards different systems types, such as WSNs [56] or WBANs [74].

### 4.8. Use Case Specific

The final method for categorisation is based upon the use case in which the attacks are being analysed. This approach is, therefore, dependant on multiple factors, including the choice of hardware, software, the network paradigm, user interaction, and most importantly the service provided. An overview of these categorisation methods by use case is presented in Figure 5.

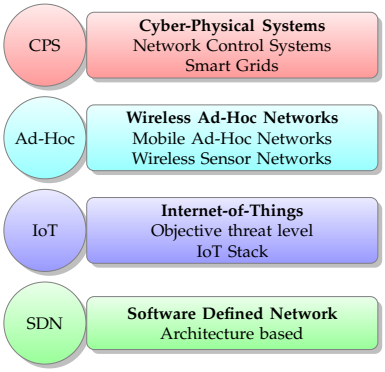


**Figure 5.** Use case categorisation methods.

#### 4.8.1. Cyber-Physical System

A Cyber-Physical System, or CPS, is defined by NIST as a device possessing interactions between both engineered components and various processes through the use of integrated physics and logic circuits [75]. Such devices can be employed in multiple areas and domains, mixing the physical world with the cyber world. For example, these devices could be employed in healthcare in elderly peoples homes to assist in every day life or could be controlled and maintained in an intensive care unit.

Due to the inherent nature of such devices, attacks directly targeting sensors or actuators can cause significant issues, making the detection of such attacks a priority [76]. An examples of such an attack is the Stuxnet worm [77] attack against the industrial control systems in a uranium enrichment plant in Iran [78]. Due to the importance of data reliability between sensors and actuators, attacks that target the integrity and authenticity of such exchanges can cause false readings, leading to actions taken under false pretences.

A sub category of CPS is the notion of Networked Control Systems, or NCS, which are highly used in various different types of Critical Infrastructures. The specially distributed systems rely on various shared networking infrastructures to allow communications between their different components, such as sensors and actuators. As such, in using communication networks, they inevitably inherit their strengths but also their weaknesses [79]. In this case, the authors of [80] decided to separate the attacks on NCS' by *attacks on physical components* or *attacks on the communication network*.

Similar to a previous approach, this method created a clear distinction between attacks that target a system device and network activities themselves. This allows the separation between attacks aiming to impact a single device, versus those whose objectives concern the communication network between all devices. However, this distinction is insufficient to clearly categorise certain attacks. This is explained in [80] where attacks on sensors can either be categorised as physical, tricking the device into transmitting incorrect data, or network related, by transmitting a false signal on behalf of the sensor. An example of an NCS attack is the assault against the Maroochy Water Services in Queensland, Australia in 2000 where a wireless network link to the wastewater pumps was exploited resulting in untreated waste being released [81].

#### 4.8.2. Smart Grids

These systems, classed as Critical Infrastructures, use various smart devices to measure the energy expenditure and adapt the grid distribution as needed. Many different threats exist towards Smart Grids, such as DoS, Replay and Jamming [82,83] as well as Network Topology Attacks, which manipulate the communications between control centres and grids to create blackouts, leading to power system disruptions.

Furthermore, many network-based attacks, such as Sniffing, War Dialling, the process of dialling random numbers until until a connection is found [84] , MitM, and FDI, can also take place on these communication links, impacting the integrity of the communications [85]. As demonstrated during the 2015 Ukraine Blackout, where multiple coordinated attacks brought down three power suppliers plunging people into darkness for several hours, attacks targetting data control links can result in severe consequences [86].

As a result, FDI attacks are considered the most dangerous in this context, with the attackers knowledge of the target environment and their level of access to said environment both influence the outcome. A method of categorisation for attacks against Smart Grids is proposed in [87], separating attacks into three distinct categories: the *Power and Energy Layer*, *Computer/IT Layer*, and *Communication Layer*. The first category, the *Power and Energy Layer*, concerns attacks against both control stations and equipment. In the case of control stations, only FDI attacks against AC and DC State Estimation, a significant central part in Energy Management Systems are considered, impacting the generation and upkeep of energy supplies.

These attacks, considered stealthy and difficult to detect can bypass standard State Estimation techniques, making them difficult to counter [88]. On the other hand, attacks against equipment aim to cause physical damage to different devices by altering operational factors, such as Inertial Attacks, by increasing the speed of heavy equipment, or even Wear Attacks, which exploit malicious commands to cause wear-and-tear on equipment, reducing their life expectancy.

The second category concerns attacks against the *Computer/IT Layer*, this time targeting the IT devices themselves running command software. The attacks here are split into two distinct sections, the first of which concerns software attacks, which take advantage of programming weaknesses. Examples of such attacks include Buffer Overflows, which consists of going beyond the memory buffers capacity to inject malicious code in active memory [89] and Dangling Pointers, which point to an invalid memory location where a data object has been deallocated but not yet deleted [90].

The other part of the *Computer/IT Layer* concerns malware attacks, such as Trojans, an inconspicuous program hiding malicious functionalities to evade security restrictions when executed [91] or Malicious Bots, a seemingly harmless intermediary program that receives commands from a third party to undertake malicious activities on the infected device or towards remote targets [92]. The third and final category evolves around the *Communication Layer*, once more targetting two aspects, the first of which is directed towards the Communication Protocols themselves. Dependant on the hardware and systems involved, various different protocols exist, such as Modbus [93] or DNP3 [94]. The

second aspect concerns network related attacks, containing some familiar faces, such as DoS, MitM, and Replay Attacks.

#### 4.8.3. Wireless Ad-Hoc Networks

Contrary to the classical functionality of wireless communications, which transit through a central infrastructure, certain devices communicate directly between each other using direct ad-hoc communications. Furthermore, it is possible to use what is known as a multi-hop network structure, where multiple network devices serve as relays between a source and destination. Wireless Sensor Networks (WSN) use small sensor devices to retrieve information and then rely on the principals of wireless ad-hoc networks to relay their data back to a central point, through multi-hop routing [95].

Due to their versatility and adaptability, they can be deployed in multiple areas from environmental applications, such as the aforementioned forest fire monitoring system, to health or home applications, such as ECG devices to monitor patients health [96]. In certain cases, these types of equipment can also possess motion, meaning their network topology is constantly fluctuating, causing the need for constant adaptation and exploration of their surroundings. These networks are called Mobile Ad-Hoc Networks, or MANETs, and are an area of research in constant exploration.

With the possibilities of multiple routing paradigms, communications between devices can be more or less prominent, meaning any attack could have a greater or lesser impact on the network functionality. Attack examples include the classic DoS, MitM, as well as Replay and Jamming. However, due to the importance of communications in such a dynamic network, attacks that directly interact with routing have increased impact. These attacks are called Byzantine Attacks, where an attacker takes control of authenticated devices on the network and exploits them to arbitrarily disrupt routing [97]. Examples of such attacks include:

- **Black-Hole Attack**, which influences routing decisions to force all messages to transit to the compromised node itself to then be dropped, resulting in a DoS of varying intensity [98].
- **Wormhole Attack**, which creates an unauthorised long distance link between two compromised nodes, forwarding data from one end of the network to the other, disrupting routing efficiency as nodes on one end believe they are closer to nodes on the other end than they are [99].
- **Gray-Hole Attack**, which functions in a similar fashion to black-hole, except, instead of dropping all passing messages, only a select few will be dropped, dependant on various metrics from random to specific message types [62].

Due to the nature of WSNs, which can be left for long durations to monitor data in remote areas, such as the previous example of forest fire monitoring systems, they are susceptible to tampering and other network-based attacks. An example of such an attack is the Sybil Attack, where an attacker forges illicit identities to incorporate illegitimate nodes directly into the network. This allows the nodes to not only relay information between nodes but also emit false sensor data, which can trick the system into believing that an actual forest fire is not happening, allowing it to grow in intensity.

A simple method of threat categorisation when multiple areas and domains are being evaluated is the separation based on the application used, in this case *Attacks on MANET* and *Attacks on WSN* as explained and presented in [20].

#### 4.8.4. IoT

Since IoT networks are becoming increasingly common, their security concerns are also increasing. Following this upwards curve in the deployment and integration of IoT devices in multiple sectors, such as Critical Infrastructures, attacks against these systems are also increasing. As such, research into this area is in constant evolution, proposing new methodologies for attack detection as well as solutions to various issues, such as the integration of blockchain methodologies into communication paradigms [100].

Due to this interest in IoT as well as their security issues, multiple categorisation methods have been proposed to cover the various attacks against such architectures. In many IoT applications, the various devices communicate directly to each other, using Machine-to-Machine (M2M) communications to share or retrieve data, such as a display device soliciting a thermometer sensor node to provide and show the temperature.

However, such networks are susceptible to multiple attacks since these communications are both self configured and maintained. Examples of these attacks [101] include DoS, MitM as well as Configuration Attacks, which use fake updates to trick users into downloading malware [102], which, in this case, employ software updates on a distant nodes, or even privacy-related attacks, such as types of eavesdropping or spoofing.

In [100], the proposed categorisation for security issues was split into three level-related categories: *Low-Level*, *Intermediate-Level*, and *High-Level Security Issues*. *Low-Level Issues* encompasses all threats against the lowest network layers, Physical and Data-Link, but also against the hardware itself. This includes such attacks as jamming, sleep deprivation, otherwise know as Denial-of-Sleep [103], which forces devices to stay awake and transmit data, causing their energy reserves to dwindle, resulting in a DoS attack [104], or a low level spoofing attack, like faking a MAC address to trick neighbours.

Moving up a level to *Intermediate-Level Security Issues*, we find all attacks against network and transport-layer-related activities, such as routing or session management. Here, we can find such attacks as Replay attacks, Sinkhole, Communication Authentication, using cryptographic keys to secure and authenticate nodes, as well as RPL routing attacks, which impact the IPv6 Routing Protocol for low power and Lossy networks (RPL) by exploiting compromised nodes to gain access to data exchange and perform multiple malicious activities [105].

The final *High-Level Issues* evolve around the applications themselves that are running on the various nodes. Such threats revolve around application vulnerabilities, such as insecure public interfaces, causing a breach to data privacy, or insecure software or firmware, allowing the attacker to take advantage of injection attacks, like SQL [68] or XML-Injection [106].

Another method for categorising IoT attacks was proposed by [13] and revolves around the three IoT stack layers *Perception*, *Network*, and *Application*. Similar to the previous approach, the layer separation allows identification of attacks depending on their impact on network operations. The *Perception* layer, also called the *Sensors* layer, concerns all operations on the sensor nodes themselves, from data collection to processing and transmission.

Attacks, such as Replay or Timing Attacks, are a type of Side-Channel Attack to extract cryptographic keys by evaluating the algorithm execution time [107]. The second category, *Network*, deals with the data exchange between devices, from routing to data transmission itself. Here, attacks, such as DoS, MitM, eavesdropping, and traffic analysis, can take place.

The final layer, *Application*, deals with the data itself, creating the "smart" environment itself, all the while protecting the data's authenticity, integrity as well as confidentiality. We can find attacks that impact the data itself, such as data injection, which can cause a large data overhead, resulting in a data overload and resulting in a DoS. However, it is important to note that, in [13], they state that no global policies or standards exist for governing application interactions and development, thus, resulting in various security issues. Ref. [108] used the same categorisation approach, all the while using different terminology for the categories based upon the Attack Vector itself: *Hardware*, *Communication Links*, and *Interfaces/Services*.

#### 4.8.5. Software Defined Networking (SDN)

With the increased deployment of IoT devices throughout the world, the concern for safety increases. Although many security mechanisms exist, such as firewalls or detection and prevention systems, they are deployed along the internet edge, protecting the enclosed

network from external attacks. However, the borderless architecture in use by IoT devices bypasses such systems and raises many security concerns. One method to combat such risks is the introduction of Software Defined Networking (SDN) to encompass and regulate routing decisions in the network itself [59].

Routing decisions are then undertaken by a global network controller that interacts directly with the SDN switch through the use of the OpenFlow protocol [109]. This paradigm can, however, be adapted to multiple types of networks. For example, an SDN architecture can be implemented over an ad-hoc network, incorporating a virtual switch into each device, through which each communication will take place [59].

With the association of WSNs and IoT in multiple areas, such as meteorology or even military surveillance, it becomes even more important to secure the various data exchanges. In [110], multiple solutions for SDN wireless-sensor-based IoT security as well as SDN-based IoT management and cellular solution frameworks have been proposed. However, like all other systems connected to the Internet, SDNs are also susceptible to various types of attack:

- Reconnaissance, where the attacker can observe and analyse various vulnerabilities in the SDN system, allowing them to possibly penetrate into the system.
- Data Exfiltration Attack, where, once the attacker has gained access to the system, they can recover and extract compromising data as well as security credentials to the rest of the system.

Attacks, such as Reconnaissance, allow an attacker to observe and analyse vulnerabilities in the SDN system, allowing them the possibility to penetrate into the system. Once inside, Data Exfiltration attacks can be used to recover compromising data as well as the extraction of system credentials. These attacks cause both the loss of integrity followed by confidentiality [111] and are two of the main data-related issues related to SDNs.

Another attack to which SDNs are also susceptible is a variation of the DoS attack, using multiple compromised botnet machines to launch large-scale simultaneous DoS attacks against a specific target, called *Distributed-DoS* (*DDoS*). Although SDNs are capable of being used for DDoS detection as well as react to and block such attacks on an SDN network [112], the SDN controllers themselves, which are the brains of such detection mechanisms, can be targeted specifically. In this case, packets can take advantage of the SDN routing paradigm, transferring all unknown packet IPs to the controller, resulting in a data overload and a DoS [113].

When it comes to SDNs, the authors of [114] proposed a categorisation method to differentiate attacks dependant on the SDN architecture layers [115], which are affected or targeted by the attack. Furthermore, they also included two inter-layer categories that corresponded to the interfaces between the upper and lower layers. These five categories were the following: *Application Layer*, *Application-Control Interface*, *Control Layer*, *Control-Data Interface*, and *Data Layer*.

The first category, *Application Layer*, corresponds to the highest architectural layer, which contains the various network applications used for network monitoring and control. On this layer are attacks concerning the applications themselves, such as unauthenticated application access, or resulting configuration errors, such as no policy or fake policy enforcement. The following category corresponds to the *Application-Control Interface*, which encompasses a collection of open source APIs, which, in-turn, englobe all communications between the *Application Layer* and the *Control Layer* below. Since this category is an interface between two layers, it is susceptible to the same application-oriented threats as the *Application Layer*.

The next category, the *Control Layer*, is defined as the most important and intelligent section of an SDN architecture. Its goal is to forward the different rules from the *Application Layer* to the *Data Layer* through the many different controllers at its disposal. Multiple threats can target this interface, including those that emerge from the previous category interface. However, new threats towards the control systems can be perceived, such as

unauthorised access or Hijacking of controllers, authentication configuration errors, and even controller-switch DoS.

The following layer is the *Control-Data Interface*, which is the connection between the *Control Layer* and the *Data Layer* through the use of various protocols. Once again, since this interface conveys data from the *Control Layer* to the *Data Layer*, it is susceptible to controller and data-related attacks.

The final category, the *Data Layer*, represents the entirety of network-forwarding devices whose rules are retrieved from the *Control Layer* through the connected interface. As such, this layer is vulnerable to the same controller and data-related attacks as previously explained, but also towards other attacks, such as flow rules or forwarding policy data leakage, or even another DoS threat, this time towards the Switch flow tables.

## 5. Analysis of the Categorisation Methodologies

In the previous section, we presented eight categorical methodologies using in the literature. Each of these categorisation techniques were explored and the various approaches were defined and explained from the standing point of their respective authors. An overview of these approaches can be seen in Table 2.

In this table, we can clearly see that some approaches have been employed more than others. For example, the Attack Type categorisation using *DoS*, *Probing*, *R2L*, and *U2R* has been used in seven different publications. However, we also notice that both the Attacker Position (*Inside*/*Outside*) and the Attacker Implication (*Active*/*Passive*) have also been used numerous times, in five and six publications, respectively. Furthermore, in taking a closer look at the publications from these two categories, we can identify that the publication [13] used both categories. This highlights the fact that, in many cases, a single categorisation technique is insufficient to both structure and organise cyber attacks.

Although each of these methodologies have proven their worth through their different publications, we hope to provide a novel analysis from the standing point of IoT applications in CIs. Certain approaches analysed here provide insufficient information as to their proper use. The first would be the Attack Severity categorisation, which organises attacks based upon the severity of their impact. However, as explained previously, their severity can vary dependent on many factors, such as system use, hardware type, or even network paradigm.

For example, categorising a jamming attack would significantly depend on the use of wireless technologies in the system. Furthermore, the severity of jamming of an IoT device would vary depending on the application of the device itself. For instance, if the device is providing temperature readings to a weather station, then jamming the data exchange results is a low severity since the data is not considered essential. On the other hand, if the device was part of a personal medical surveillance device, such as a pacemaker or smart insulin pump, jamming the exchange between the device and the hospital servers could result in severe consequences for the patient, making the severity sky rocket.

The second categorisation of issue is the **Wireless Ad-Hoc Networks-Use-Case Specific** approach. Their usage of simply separating attacks, such as targeting MANETs or WSNs, does not provide any precise information regarding the attacks themselves. This is only useful if covering multiple types of wireless direct networks; however, to be able to structure attacks in a more detailed way, other approaches must be used in tandem.

When analysing IoT devices that are constantly communicating with the outside world, the use of a **Network-Layer-Oriented** approach is appealing. Using this approach, all network-based attacks can be organised depending on the layer in which they occur. However, the limitation of this approach is just that: network-based attacks.

**Table 2.** Overview of the categorisation methods.

| Categorisation | Approach | References |
| --- | --- | --- |
| Attack Severity | Six threat levels: Localised, Moderate, Substantial, Significant, Highly Significant and National Cyber Emergency | [15] |
| Access Type | Physical, Cyber | [16] |
| Attack Type | DoS, Probing, R2L, U2R | [19–25] |
| | DoS, MitM, Brute Force | [26,30] |
| | DoS, Replay, Deception | [35,36] |
| | Active Eavesdropping, Scanning, Probing | [44] |
| | Physical, Network, Software, Encryption | [55] |
| Attacker Position | Outside, Inside | [13,56–59] |
| Attacker Implication | Active, Passive | [13,20,56,60–62] |
| Objective Oriented | Privacy | [16] |
| | Reconnaissance, Access, Malicious, Non-Malicious, Cyber Crime, Cyber Espionage, Cyber Terrorism, Cyber War | [20] |
| | Disconnection and Goodput Reduction, Side-Channel Exploitation, Covert-Channel Exploitation | [44] |
| | Hardware, Network, Human Factor | [57] |
| | Interception, Interruption, Fabrication, Modification | [61] |
| | Access Control, Authentication, Availability, Confidentiality, Integrity | [70] |
| Network Layer Oriented | OSI model, Layers 1–4 and 7 | [56,74] |

**Table 2.** *Cont.*

| Categorisation | | Approach | References |
|---|---|---|---|
| Use-Case Specific | CPS-NCS | Attacks on Physical Components, Attacks on Communication Network | [80] |
| | CPS-Smart Grids | Power and Energy Layer, Computer/IT Layer, Communication Layer | [87] |
| | Wireless Ad-Hoc Networks | Attacks on MANET, Attacks on WSN | [20] |
| | IoT | Low-Level, Intermediate-Level, High-Level Security Issues | [100] |
| | | IoT Stack Layers-Perception, Network, Application | [13,108] |
| | SDN | SDN Architecture-Application Layer, Application-Control Interface, Control Layer, Control-Data Interface, Data Layer | [115] |

In many cases, especially in IoT applications where devices are left alone or provided to individuals, such as our previous medical example, physical tampering is also a significant risk. Not only can the device itself be damaged or broken, but, with direct access, attackers can analyse the system in detail, providing them with a significant edge. Furthermore, certain software related threats, such as Viruses, Data-injection, and Ransomware, are all categorised upon the Application layer, without further detail as to their organisation.

One of the most common used approaches, **Attacker Implication**, grants an important insight into the use of the attack, such as separating reconnaissance threats from malicious activities. However, alone it is insufficient to provide enough input to properly categorise and separate attacks. As stated previously, this approach is used alongside other approaches. As such, it is a good method for providing further insight to certain methods, such as the previously explored **Network Layer** approach, allowing for each network layer to be separated into passive and active attacks.

Overall, each of these methods possess their own merits since they can be used at the authors discretion to represent attacks how they see fit. However, when coupled with the large number of categorisation approaches, this can lead to confusion in understanding the structure but also as to which is the best approach to employ. Thus, we hope to provide insight into some of the methods and approaches used in the literature to inform and help guide in the choice for a suitable solution.

## 6. Discussion

The use of categorisation methods allows specialists to organise threats to their systems in such a way that allows ease of access and understanding. However, they also contribute towards the advancement of adaptive and robust solutions through their structuring of different attacks.

It is important to note that that there are many types of systems that are not covered in this survey. The adoption of machine learning techniques on both sides of the fence, as well as the use in other systems can impact how threats are perceived, as well as their target. An example of such a system would be an extension of the aforementioned CPS, where machine learning techniques are incorporated directly into the control circuitry, making the system itself a "Smart-CPS" but also opening the system up to further threats. This notion is just a portion of a vast category, engulfing many emergent technologies and methods, which necessitates its own in dependant analysis.

In this section, we will present and discuss two cyber security notions that also contribute towards these elements. First, we will discuss some of the various **challenges** faced by *Intrusion Detection Systems (IDS)* as well as IoT devices and networks. Secondly, we will glance at some of the available **data sets**, which can be used in tandem to efficiently test solutions for some of the aforementioned challenges.

### 6.1. Challenges

Many challenges exist when it comes to cyber security, generally residing around the various threat detection techniques and system vulnerabilities. As such, research in this area strive to analyse as well as provide answers towards many of these issues. However, these challenges also extend to a research point of view where the advancement of new attack techniques cause research difficulties to be overcome. Some of these challenges, explained in [57], revolve around the detection capabilities of various systems, since encrypted data or networks increase the complexity of detection methods.

Novel attack methodologies, like remote hardware attacks, which are possible through the use of software attacks, such as Rowhammer [116], increase the need for adaptive and robust detection methods, since access to the hardware was previously necessary for such attacks. Finally, they mention the type of architecture needing protecting since Industrial System detection methods are not easily transferable to the various IoT network variants and implementations.

#### 6.1.1. Intrusion Detection Systems

In [21], the authors defined the various challenges revolving around Intrusion Detection Systems (IDS), in particular around the protection of Industrial Control Systems and the use of Intrusion Evasion Detection. In the former, the unique architecture and operational importance of Industrial Control Systems cause complications for IDS due to the different attack variants. In various cases, many systems use outdated Microsoft Legacy operating systems, which increase the complexity the protect these patch-less zero-day vulnerable systems.

An historical example of such issues is the WannaCry Ransomware, which devastated the National Health Service in the United Kingdom, where many of the systems were still running unprotected Windows XP [117]. The other challenge of IDS, the use of Intrusion Evasion Detection techniques, complicates attack detection by the use of evasion methods by attackers to mask their attacks. This complicates the detection of the attack signature but also the creation of an after-event signature to complement the attack detection arsenal, impacting the robustness of IDS when facing evasion techniques.

#### 6.1.2. IoT

Along with the previously presented increase in security concerns with the development and wide scale deployment of IoT networks, many questions and challenges arise. Since the goal of these devices is to be left alone for long periods of time, protecting them when each IoT stack layer is susceptible to attack is an ongoing challenge. In [13], along with their previously defined categorisation in Section 4.8.4, the authors presented the difficulties towards threat and attack detection as well as some of the threats towards their operation.

For example, the use of wide-scale wireless signals on the perception layer leaves place for disruption and jamming attacks, which, when coupled with the device being in a remote outdoor location makes them easily accessible to the attacker. Furthermore, the inherent machine-to-machine communications presented previously also identifies the issue of compatibility between devices. These compatibility problems also extend to the Application layer, where, due to the previously stated lack of development standards for applications, further issues can arise. These challenges are some of the many layer-related challenges with which detection methods are confronted, orienting further research into these areas.

With the increase in IoT diversity within different network structures, increasing vulnerabilities may appear. Indeed, as raised in [118], increasing the number of devices increases the possibility of vulnerabilities. However, by increasing the number of different devices present, this risk raises exponentially due to the level of complexity between devices. A single device type may poses a certain vulnerability, but by quelling this weakness, all devices derived from this type will also be secured.

On the other hand, by adding more device variety into the mix, these vulnerabilities become both harder to detect and plug. Furthermore, with the mass deployment of certain types of IoT devices, such as sensors, any common vulnerabilities become amplified due to their large numbers and common application uses. Other risks increase with larger numbers of devices in a network related to intercommunication where the number of interconnection possibilities increase exponentially putting a strain on device to device security, such as limited device authentication. These limits make it easier for attacks to infiltrate the network undetected by compromising a device directly or including a new device into the mix, which thereafter bestow havoc therein.

Another key challenge for IoT devices as analysed by the authors of [118], revolves around their interoperability. Indeed, many different characteristics, which make such gadgets what they are, also contribute towards their limitations. We spoke previously about limited authentication methods between devices, but this is also valid from an application view point.

When coupled with the use of embedded password on devices for administrative purposes, any compromised node will not only grand the attacks access to the network but

potentially the admin passwords for the rest of the network. The autonomous nature of IoT devices is one of the strong selling points, as they can be deployed in remote areas and accomplish their tasks unsupervised. However, this automatic functionality can be taken advantage of by tricking the devices to access compromised or malicious remote servers, thus, allowing the attacker to enter the network.

This is increased by the lack of proper device monitoring or remote access administration, since, in many remote cases, such as battlefield sensor deployment, such notions are impossible to achieve. However, when they are possible, they are somewhat limited, due to the lack of security policy upkeep for both device monitoring and the wireless network protocol used for remote access. The attacker can, therefore, exploit this weakness to compromise a device, all the while sending false information back to the monitoring station, tricking the remote administrators into believing that all is well.

Finally, like any device connected to the internet, OS and application security patches are quintessential for device security. However, in many cases, these updates take considerable time to reach the devices, giving any malicious third party time to exploit the unpatched vulnerability, which, when coupled with the use of unauthenticated third-party applications, increase the chance of malicious interactions in the network.

As presented previously in Section 3.2, the authors of [14] presented the various features of IoT networks as well as some of their associated threats. However, they also identified some of the security challenges associated with each feature as presented in Figure 6.

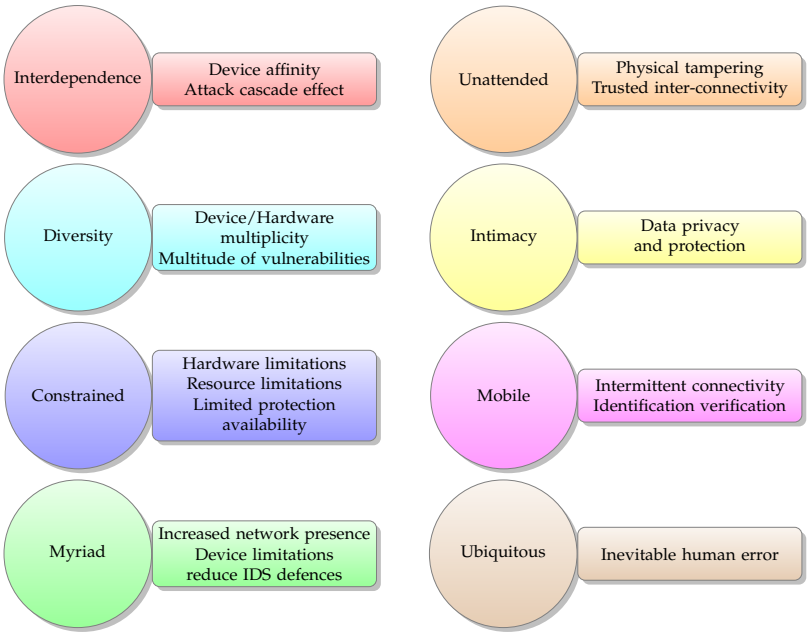


**Figure 6.** IoT security challenges.

Interdependence

This interdependence is somewhat underestimated and underevaluated in the scientific community. Indeed, many efforts are directed towards protecting a single device, not taking into account that a smart plug could potentially cause a chain of events resulting in a open window. Unfortunately, this interdependent behaviour makes it difficult to implement security methods, making measures, such as defensive boundaries and static access control methods difficult to enact. Furthermore, since devices, such as sensors, rely on external stimuli to function, permission rules become difficult to fine tune due to the unpredictable nature of the environment. As such, the authors of [14] identified that overprivilege in such applications has become a common problem.

Diversity

Due to the large diversity of devices used in a single IoT network, designing a single defence system revolving around multiple technical specifications is extremely complicated. Indeed, as stated previously, the possible number of vulnerabilities increase with large number of devices, even more so when multiple types of devices are used. Furthermore, different devices use different network protocols to function, each with their own unique specifications and risks. This means that research efforts must be directed towards the consequences of such diversity, such as addressing the many vulnerabilities that arise as well as the numerous risks associated with multiple network protocols used in the network.

Constrained

The constrained nature of IoT devices limits their effective functionality to a few distinct applications. However, these applications generally revolve around the capture and dissemination of data between devices, meaning that efforts must evolve around protecting these limited resources. Unfortunately, these hardware constraints also impact the protection of these devices, as creating security measures with limited resources is an ongoing challenge. Furthermore, employing complex cryptographic encryption methods and authentication algorithms are also a challenge, due to the latency and resource consumption issues of these small IoT devices.

Myriad

The increasingly large number of devices employed in IoT networks as well as large quantities of shared data was referred to as "Myriad" by the authors of [14]. Increasing the quantity of devices functioning in tandem increases security risks due to their constrained and unique technological nature. This means that conventional defensive systems will not operate in essentially a severely limited hardware environment. Unfortunately, the lack of IoT-specific IDS or system defence tools, such as anti-viruses or anti-malware, severely impacts the security of these devices. Indeed, detecting and stopping the spread of botnet viruses with limited resources and tools is a significantly difficult challenge.

Unattended

The ability to leave a device in a remote area unattended is one of the strong points for IoT devices where surveillance is needed, such as weather applications in agriculture or battlefield surveillance for the military. Even with their constraints, each device is created to perform a specific task all the while adhering to its limitations, in particular its limited energy reserves. As such, as stated previously, conventional defence systems will not work on limited systems. Furthermore, securing the device against tampering is a significant challenge, both on the physical side but also the hardware itself due to the characteristic of the onboard systems. This results in more attention turning towards defining a secure and trusted execution environment to reduce the risk of device exploitation.

Intimacy

As explained previously, the intimate nature of the relation between user and device gives way to many privacy-related challenges. With increasing large scale applications, such as smart cities collecting and manipulating personal information as described in [119], private data is increasingly at risk of exposure. For example, personal data is being used more for independent third party services, such as logging into a website using a social media account, sharing the data between the two platforms. This sharing although granting authentication to the user, increases the chances of a privacy leak.

As such, many IoT Intimacy related challenges evolve around how such data is captured as well as how it is used and shared [120]. With biometric and GPS chips in many portable IoT devices, users are able to be identified as well as localised and even tracked with or without their knowledge. Furthermore, with increasing devices sharing our day to

day lives, they are capable of capturing and correlating large quantities of data, effectively generating an identity profile of the user.

This can, in turn, be exploited to specifically target the user's interests, as with targeted advertisements, or even to use social-engineering techniques to infiltrate IT systems. These are significant privacy issues where data is being captured and used without the users knowledge or express authorisation, and even, in some cases, the data is sold to another entity, once again forming a significant breach of privacy, As such, a significant challenge towards IoT intimacy and privacy is to find the middle ground between capturing, sharing, and using sensitive data; and their protection.

Mobile

One of the final features of IoT networks is the mobility of devices. Although this mobility grants many possibilities, it also raises some security challenges concerning its operability. For example, moving can cause a device to disconnect from a known domain and connect to another, previously unknown. Thus, the device needs to be verified before allowing access to the network as well as granting it various permissions to interact with the network services.

However, verifying devices and deciding the correct permissions is a difficult task, since identifying a device as legitimate is an ongoing challenge in multiple areas. Furthermore, not only must the devices identity be verified but also any data it carries must be secured when switching network domains since confidential material may be present. As such, data confidentiality must be maintained and, in the case of data encryption, key negotiation must be secured.

Ubiquitous

The threats towards the "Ubiquitous" nature of IoT devices as presented by the authors of [14] generally revolve around human error. As such, there are no specific challenges towards such a feature since human error is inherently inevitable. Many of these errors are the result of accidental manipulation or configuration due to a lack of education and awareness, a notion that is examined in [57].

That being said, certain steps can be taken to help limit these risks, such as manufacturer and professional operator training to reduce the possibility of misconfiguration. However, when it comes to the general consumer, such training is not possible. The only option is risk sensitisation through professional workshops to sensitise during work hours, or to include basic security awareness sessions into a university or high-school curriculum.

### *6.2. Data Sets*

To be able to correctly and accurately train and use IDS, attack data must be used. Thankfully, many threat data sets exist that can be used for such efforts. Each data set contains traces for specific uses, such as individual attacks or extracted in specific scenarios. However, as presented in [21], access to such data sets is often difficult due to the limited availability of publicly accessible collections when compared to private restricted versions. Furthermore, the use of these public data sets comes with the risk of invalid data input contained in the sets that could influence the outcome of IDS.

Here, we present an overview of available cyber attack data sets by taking a closer look at various characteristics and features of the sets themselves. First, however, we explain the choice of categories used tor this analysis as presented in Figure 7 as well as the importance of analysing the different features.

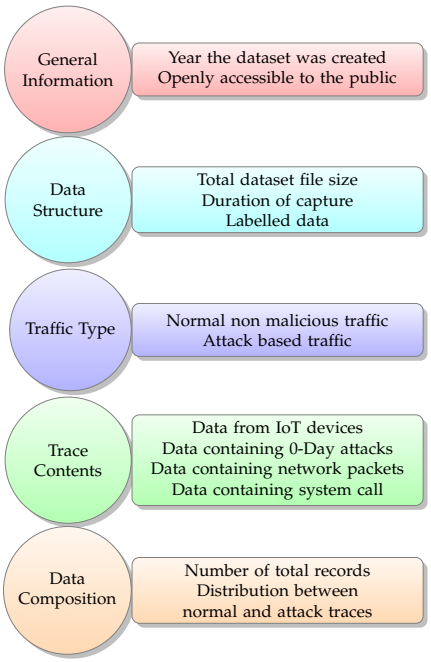


**Figure 7.** Dataset features.

#### 6.2.1. General Information

The first element we analyse from the different data sets is what we call General Information regarding the data set itself as well as the governing body. In this category, we take a look at the year in which the data set was created as well as if the data set is publicly available. In the former, extracting the different dates from each recorded data set grants a significant insight towards the contents of the set without needing access. Indeed, many attacks are time sensitive, meaning they either were very common many years ago, or are new discoveries in recent years. In either case, a 2-month-old data set will not contain the same information as a 20-year-old one, simply due to the advancements in networking and system architecture as well as security measures and attack methodologies.

The other general characteristic, which we named 'Public', allows us to separate publicly accessible data sets from private ones. Furthermore, we took this one step closer by also noting the data sets for which public access is available, but only to academic or research entities through the means of a request form. In some cases, data sets may be used in commercial situations, however, permission from the maintainers is also needed. These specifications towards public use have been included in our analysis.

#### 6.2.2. Data Structure

The second element of interest concerns a brief overview of the data contents and structure. Since many data sets contain significant trace elements for use in IDS, their size can vary. This is, therefore, the first element that we analyse since data set size is in direct correlation to both the complexity and density of the overall contents. However, a larger data set does not imply diversity in the trace contents, which we analyse at a later date.

An element that is linked to the data set size, however, is the time frame during which the data set was constructed. We called this category 'Duration'. As explained, we note the time frame as specified by the data sets creators, which grants an insight into the quantity and potential complexity of trace data. This allows the possibility to differentiate between a large file size but short timespan, meaning a dense data capture from a smaller, larger timespan, meaning a more diverse but limited data features.

One important feature used in data sets is the incorporation of labels, allowing IDS the ability to identify a specific data point as belonging to a certain type of action. This is generally used to separate 'Normal' traffic from 'Attack' traffic, reducing the complexity

of machine learning based detection systems by allowing to train them from known traffic types.

#### 6.2.3. Traffic Type

However, in some cases, only one type of traffic is included in a data set. The two main types we take into account are the notion of 'Normal' traffic, which we assimilate to everyday routine operations, and 'Attack' traffic, which we consider to be abnormal or unusual operations. Some data sets only provide traffic pertaining to either one category or the other, meaning the detection system itself must be capable of differentiating abnormal behaviour. In the first case, a detection system can perceive abnormal traffic as a threat, the second when trained from attack data means detection systems possess only a glimpse into abnormal behaviour, and in many cases only a small extract belonging to specific attack methodologies.

#### 6.2.4. Trace Contents

With an overall idea of the data set information and data structure, an important characteristic is the trace category to which the data points belong. By this, we mean what sort of data is contained in the data set, separating from use case to target system. The first two categories we differentiate are 'System' and 'Network'. Here, we can identify if a data set contains traces that concern operating system calls or network-based threats.

Although these two categories cover almost all types of threats perceived in the cyber domain, another category is extremely important when looking at cyber attack detection. The notion of 'Zero-Day' (or '0-Day') attacks concern any threat that takes advantage of a new vulnerability before it has been properly patched. This means that many 0-Day attacks do not possess accurate trace data that can be used for detection. However, some data sets use different methods, such as previous 0-Day traces to train detection systems into picking up new exploits and reducing the severity of the impact until the weakness can be repaired.

The final category and a point of interest in this survey, is the notion of IoT attack traces. Indeed, many data sets are generated from either real or simulated environments; however, they all revolve around normal network architecture or devices. With the expansion of IoT into the real world, new vulnerabilities are forged, meaning that different threats can target these systems with more ease. Furthermore, the specific nature of IoT devices means IDS must be trained in the specific protocol exchanges between IoT points.

#### 6.2.5. Data Composition

The final category that we use in our analysis is what we call the Data Composition. Here, we take a close look at the contents themselves, in particular the separation between normal and attack traces, if both are present. This allows us to identify data sets that are more oriented towards providing attack traces for IDS to analyse then normal traces, allowing detection systems to grasp what we call 'Normal 'operations. This also allows us to rebound on some pointers from our analysis on the data structure, by correlating the size of the set and the number of entries. Here, we can see data sets that possess large quantities of features per data set trace with fewer number of entries, compared to larger numbers of entries meaning less features.

#### 6.2.6. Data Set Analysis

In Table 3, we present an overview of 40 data sets, some of which were identified from [21,121]. The resulting table format was inspired from their own analyses, adding our own touch to the organisation. As specified in [122], in certain cases, an existent data set does not fulfil the expectations of specific expectations. As a consequence, some researchers have created their own 'data sets 'to be used with their own research and their specific use cases.

**Table 3.** Overview of intrusion detection data sets.

| Data Set | Information | | Data | | Traffic Type | | | Trace Contents | | | | Data Composition | | | References |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Year | Public | Size | Duration | Labelled | Normal | Attack | IoT | 0-Day | Network | System | Nb Records | % Normal | % Attack | |
| ADFA-LD | 2014 | ✔ | 2.3 MB. | ✳ | ✔ | ✔ | ✔ | ✘ | ✔ | ✔ | ✔ | ✳ | ✳ | ✳ | [123–126] |
| ADFA-WD | 2014 | ✔ | 29.6 MB. | ✳ | ✔ | ✔ | ✔ | ✘ | ✔ | ✔ | ✔ | 1,033,233 | 64% | 36% | [125,126] |
| ADFA-WD:SAA | 2014 | ✔ | 403 MB. | ✳ | ✔ | ✔ | ✔ | ✘ | ✔ | ✔ | ✔ | ✳ | ✳ | ✳ | [125,126] |
| AWID | 2015 | ✔* | ✳ | 108 h. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | 210,900, 113 | 97% | 3% | [127,128] |
| Booters | 2013 | ✔ | 250 GB. | 2 d. | ✘ | ✘ | ✔ | ✘ | ✘ | ✔ | ✘ | ✳ | 0% | 100% | [129] |
| Bot-IoT | 2018 | ✔? | 69.3 GB. | ✳ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✘ | 72,000,000 | ✳ | ✳ | [130,131] |
| Botnet | 2014 | ✔* | 13.8 GB. | ✳ | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | ≈915,944 | 69% | 31% | [132,133] |
| CAIDA | 2007 | ✔* | 21 GB. | 1 h. | ✘ | ✘ | ✔ | ✘ | ✘ | ✔ | ✘ | ✳ | 0% | 100% | [134,135] |
| CIC-DDoS 2019 | 2019 | ✔* | ✳ | 2 d. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | ✳ | ✳ | ✳ | [135,136] |
| CIC DoS | 2017 | ✔* | 4.6 GB. | 24 h. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | ✳ | ✳ | ✳ | [137,138] |
| CICIDS 2017 | 2017 | ✔* | 51.1 GB. | 5 d. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | ✳ | ✳ | ✳ | [139,140] |
| CIDDS-001 | 2017 | ✔ | 380 MB. | 28 d. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | ✳ | ✳ | ✳ | [141,142] |
| CIDDS-002 | 2017 | ✔ | 200 MB. | 14 d. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | ✳ | ✳ | ✳ | [141–143] |
| CDX | 2009 | ✔ | 12 GB. | 4 d. | ✘ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | ✳ | ✳ | ✳ | [144,145] |
| CTU-13 | 2013 | ✔ | 697 GB. | 143 h. | ✔ | ✔ | ✔ | ✔ | ✘ | ✔ | ✘ | 20,643,076 | 98% | 2% | [146,147] |
| DARPA | 1999 | ✔ | ✳ | 25 d. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✔ | ✳ | ✳ | ✳ | [148,149] |
| Gure KDD Cup | 2008 | ✔* | 13.6 GB. | 35 d. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | 2,759,494 | 41% | 59% | [150–152] |
| IRSC | 2015 | ✘ | ✳ | ✳ | ✔ | ✔ | ✔ | ✘ | ✳ | ✔ | ✘ | ✳ | ✳ | ✳ | [153] |
| ISCX 2012 | 2012 | ✔* | 84.4 GB. | 7 d. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | ✳ | ✳ | ✳ | [154,155] |
| ISOT | 2010 | ✔* | 420 GB. | 3 mnth. | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | ✔ | 1,675,424 | 97% | 3% | [156,157] |
| KDD CUP 99 | 1998 | ✔ | 743 MB. | ✳ | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✔ | 4,898,431 | 20% | 80% | [151,158–160] |
| Kent 2016 | 2016 | ✔* | 12 GB. | 58 d. | ✘ | ✔ | ✳ | ✘ | ✘ | ✔ | ✔ | 1,648,275,307 | ✳ | ✳ | [161,162] |
| Kyoto 2006+ | 2006 to 2015 | ✔ | 19.2 GB. | 10 y. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | ✳ | ✳ | ✳ | [163,164] |
| LBNL | 2005 | ✔ | 11 GB. | 4 mnth. | ✘ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | ✳ | ✳ | ✳ | [165,166] |
| NDSec-1 | 2016 | ✔ | 869.2 GB. | ✳ | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | ✳ | ✳ | ✳ | [167,168] |
| NGIDS-DS | 2016 | ✔ | ✳ | 27 h. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✔ | 90,054,160 | 99% | 1% | [169] |

**Table 3.** *Cont.*

| Data Set | Information | | Data | | Traffic Type | | | Trace Contents | | | | Data Composition | | | References |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Year | Public | Size | Duration | Labelled | Normal | Attack | IoT | 0-Day | Network | System | Nb Records | % Normal | % Attack | |
| NSL-KDD | 1998 | ✔ | ❋ | ❋ | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✔ | 5,209,458 | 20% | 80% | [151,158,159, 170] |
| PU-IDS | 2015 | ❋ | ❋ | ❋ | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✔ | 198,904 | 47% | 53% | [171] |
| PUF | 2018 | ❋ | ❋ | 3 d. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | 298,463 | ❋ | ❋ | [172] |
| SANTA | 2014 | ✘ | ❋ | ❋ | ✔ | ✔ | ✔ | ✘ | ✔ | ✔ | ✔ | ❋ | ❋ | ❋ | [173] |
| SSENET-2011 | 2011 | ❋ | ❋ | 4 h. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | ❋ | ❋ | ❋ | [174] |
| SSENET-2014 | 2014 | ❋ | ❋ | 4 h. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | ❋ | ❋ | ❋ | [175] |
| SSHCure | 2014 | ✔ | 2.5 GB. | 2 mnth. | ✔ | ✘ | ✔ | ✘ | ✘ | ✔ | ✔ | ❋ | 0% | 100% | [176,177] |
| TRAbID | 2017 | ✔ | 129 GB. | 8 h. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✔ | 469,442,290 | 93% | 7% | [178,179] |
| TUIDS | 2012 | ✔e | 65.2 GB. | 14 d. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | 833,006 | 52% | 48% | [180] |
| Twente | 2008 | ✔ | ❋ | 6 d. | ✔ | ✘ | ✔ | ✘ | ✘ | ✔ | ✘ | ❋ | 0% | 100% | [181,182] |
| UGR'16 | 2016 | ✔ | 236 GB. | 6 mnth. | ✔ | ✔ | ✔ | ✘ | ✘ | ✔ | ✘ | ≈16.9 B. | ❋ | ❋ | [183,184] |
| UNIBS-2009 | 2009 | ✔e | 27 GB. | 3 d. | ✘ | ✔ | ✘ | ✘ | ✘ | ✔ | ✘ | ❋ | 100% | 0% | [185,186] |
| Unified Host and Network | 2017 | ✔* | 150 GB. | 90 d. | ✘ | ✔ | ✘ | ✘ | ✔ | ✔ | ✔ | ❋ | 100% | 0% | [187,188] |
| UNSW-NB15 | 2015 | ✔ | 100 GB. | 31 h. | ✔ | ✔ | ✔ | ✘ | ✔ | ✔ | ✔ | 2,540,044 | 87% | 13% | [159,189,190] |

✔* = on request, ✔e = email contact needed, ✔? = commercial use with permission, ❋ = no information found.

## 7. Lessons Learned

During the redaction of this survey, many issues were identified. The first and foremost of them, is the presence of different categorisation methods as well as multiple approaches per method. This large diversity in options as well as the occasional lack of structure in the literature can cause some confusion to readers. The goal of this survey, therefore, was to facilitate the study of these categorisations, allowing an overview of multiple variations in a single document. This also grants the possibility to conduct further studies into areas of interest, thus, helping researchers in their choices and understanding of different categorisation techniques.

Furthermore, the choice of categories is naturally at the authors discretion, meaning that, in some cases, a brand new approach was proposed. Although this contributes to the area of cyber security, it also adds complexity due to the numerous options. This is easily identified when looking closer at specific use cases or areas of interest. For example, when structuring attacks against IoT presented previously and visible in Table 2, the authors of [100] chose to use an approach based on the threat security level. This method in our opinion, although sufficient to structure attacks, does not provide the clarity needed during reading.

The main issue is the choice of categories, since the threat security level is not only dependant on the specific use case but also on the opinion of those who created it. This remark is similar to the method Attack Severity, where the impact of each attack is not the same dependant on the system and the expert concerned. An example would be the category used to represent an "Eavesdropping" attack where one person may consider it a low level threat, whereas another might see it a significant risk to system integrity and, thus, list it as a high level threat instead.

Finally, during the evaluation and study of the various data sets, the notion of ease of access was raised. Indeed, as stated previously, many data sets provide one or more external readme files, providing insight into the contents and structure of the data sets. However, many of these providers include this readme directly into the data set archive itself, meaning that the entirety of the data set must be acquired in order to access the readme. The structure of this readme also varies dependant on the data set, providing different types of information each time.

In some cases, the readme gave information regarding the number of entries as well as decomposition between "normal" and "attack" entries or even a listing of attacks and structure information. In others, this information generally revolved around the global aspects of the data set, such as how it was achieved, its goals, a vague overview of the contents, such as a tcpdump taken over multiple days. Finally in some cases, no readme file was provided leaving the understanding of the document up to the reader themselves, which, in many cases, made it difficult to understand the structure of the data set.

## 8. Conclusions

In this paper, we presented and analysed different attack categorisation methods used in the literature. We first explored these categories, presenting them from a neutral standpoint, basing our analysis upon how they were used by the various authors. We then took an objective look at them from within the context of IoT wireless devices in use in the various areas of Critical Infrastructures. This novel approach provided not only a detailed overview of the various methodologies in use to present and define cyber attacks but also an analysis based upon their strengths and weaknesses for use in CI security.

We also provided a detailed discussion into some of the many challenges encountered with cyber security detection methods as well as the difficulties related to security principles in IoT applications. We concluded our discussion with an analysis of data sets from a novel standing point through the analysis of the data set description information provided by the different creators. This provides an overview of their basic information as well as some application uses, without the need for direct access or advanced statistical analysis.

**Author Contributions:** E.S. lead work. V.L. and N.M. equally supervised and contributed to the paper. All authors have read and agreed to the published version of the manuscript.

**Funding:** This work was partially supported by a grant from CPER DATA and by the European Union's Horizon 2020 Project 'CyberSANE' under Grant Agreement No. 833683 addressing the topic SU-ICT-01-2018.

**Institutional Review Board Statement:** Not applicable.

**Informed Consent Statement:** Not applicable.

**Data Availability Statement:** Not applicable.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. CSRC. Glossary-Cyber Attack Definition. 2010. Available online: https://csrc.nist.gov/glossary/term/Cyber_Attack (accessed on 26 August 2020).
2. McCurry, J. South Korean nuclear operator hacked amid cyber-attack fears. *Guardian* **2014**. Available online https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack (accessed on 2 August 2021)
3. Perlroth, N.; Krauss, C. A cyber attack in Saudi Arabia failed to cause carnage, but the next attempt could be deadly. *Independent* **2018**. Available online: https://www.independent.co.uk/news/long_reads/cyber-warfare-saudi-arabia-petrochemical-security-america-a8258636.html (accessed on 2 August 2021).
4. Huntsman. Critical Infrastructure Cyber Security Solutions. 2015. Available online: https://www.huntsmansecurity.com/industries/critical-infrastructure/ (accessed on 17 December 2020).
5. Viganò, E.; Loi, M.; Yaghmaei, E. Cybersecurity of critical infrastructure. In *The Ethics of Cybersecurity*; Springer: Cham, Switzerland, 2020; pp. 157–177.
6. Vanhoef, M.; Piessens, F. Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2. In Proceedings of the 24th ACM Conference on Computer and Communications Security (CCS), Dallas, TX, USA, 30 October–3 November 2017
7. Zhang, L.; Ding, G.; Wu, Q.; Zou, Y.; Han, Z.; Wang, J. Byzantine Attack and Defense in Cognitive Radio Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1342–1363. [CrossRef]
8. Rodofile, N.R.; Radke, K.; Foo, E. Framework for SCADA Cyber-Attack Dataset Creation. In Proceedings of the Australasian Computer Science Week Multiconference, Geelong, Australia, 30 January–3 February 2017.
9. Sanghvi, H.; Dahiya, M. Cyber reconnaissance: An alarm before cyber attack. *Int. J. Comput. Appl.* **2013**, *63*. [CrossRef]
10. CSRCN. Glossary-Vulnerability Definition. 2018. Available online: https://csrc.nist.gov/glossary/term/vulnerability (accessed on 26 August 2020).
11. Sullivan, J.E.; Kamensky, D. How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid. *Electr. J.* **2017**, *30*, 30–35. [CrossRef]
12. Joaquín, R. CIPSEC-Most Common Attack Vectors over Critical Infrastructures. 2018. Available online: https://www.cipsec.eu/content/most-common-attack-vector-over-critical-infrastructures (accessed on 26 August 2020).
13. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015; pp. 336–341.
14. Zhou, W.; Jia, Y.; Peng, A.; Zhang, Y.; Liu, P. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet Things J.* **2019**, *6*, 1606–1616. [CrossRef]
15. New Cyber Attack Categorisation System to Improve UK Response to Incidents. 2018. Available online: https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents (accessed on 23 September 2020).
16. Giraldo, J.; Sarkar, E.; Cardenas, A.A.; Maniatakos, M.; Kantarcioglu, M. Security and Privacy in Cyber-Physical Systems: A Survey of Surveys. *IEEE Des. Test* **2017**, *34*, 7–17. [CrossRef]
17. Smith, R. Assault on California Power Station Raises Alarm on Potential for Terrorism. *Wall Street J.* **2014**. Available online: https://www.wsj.com/articles/SB10001424052702304851104579359141941621778 (accessed on 4 August 2021).
18. Wood, A.D.; Stankovic, J.A. Denial of service in sensor networks. *Computer* **2002**, *35*, 54–62. [CrossRef]
19. Ahmed, M.; Mahmood, A.N.; Hu, J. A survey of network anomaly detection techniques. *J. Netw. Comput. Appl.* **2016**, *60*, 19–31. [CrossRef]
20. Raiyn, J. A survey of cyber attack detection strategies. *Int. J. Secur. Appl.* **2014**, *8*, 247–256. [CrossRef]
21. Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J. Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges. *Cybersecurity* **2019**, *2*, 20. [CrossRef]
22. Ahmed, M. Intelligent Big Data Summarization for Rare Anomaly Detection. *IEEE Access* **2019**, *7*, 68669–68677. [CrossRef]
23. Diro, A.A.; Chilamkurti, N. Distributed attack detection scheme using deep learning approach for Internet of Things. *Future Gener. Comput. Syst.* **2018**, *82*, 761–768. [CrossRef]

24. Stiawan, D.; Idris, M.Y.; Malik, R.F.; Nurmaini, S.; Alsharif, N.; Budiarto, R. Investigating Brute Force Attack Patterns in IoT Network. *J. Electr. Comput. Eng.* **2019**, *2019*, 1–13. [CrossRef]
25. Mahfouz, A.M.; Venugopal, D.; Shiva, S.G. Comparative Analysis of ML Classifiers for Network Intrusion Detection. In *Fourth International Congress on Information and Communication Technology*; Springer: Singapore, 2020; pp. 193–207.
26. Conti, M.; Dragoni, N.; Lesyk, V. A Survey of Man In The Middle Attacks. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2027–2051. [CrossRef]
27. Whalen, S. An Introduction to Arp Spoofing. Node99 [Online Document]. April. 2001. Available online: http://index-of.es/Networking/arpspoof.pdf (accessed on 2 August 2021).
28. Kim, H.; Huh, J. Detecting DNS-poisoning-based phishing attacks from their network performance characteristics. *Electron. Lett.* **2011**, *47*, 656–658. [CrossRef]
29. CSRCN. Glossary-Brute Force Attack Definition. 2018. Available online: https://csrc.nist.gov/glossary/term/brute_force_attack (accessed on 21 September 2020).
30. Singh, J.; Kaur, S.; Kaur, G.; Kaur, G. A Detailed Survey and Classification of Commonly Recurring Cyber Attacks. *Int. J. Comput. Appl.* **2016**, *975*, 8887. [CrossRef]
31. Rughoobur, P.; Nagowah, L. A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare. In Proceedings of the 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), Dubai, United Arab Emirates, 18–20 December 2017; pp. 811–817.
32. Yang, Q.; An, D.; Min, R.; Yu, W.; Yang, X.; Zhao, W. On Optimal PMU Placement-Based Defense Against Data Integrity Attacks in Smart Grid. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 1735–1750. [CrossRef]
33. Liu, Y.; Ning, P.; Reiter, M.K. False Data Injection Attacks against State Estimation in Electric Power Grids. *ACM Trans. Inf. Syst. Secur.* **2011**, *14*, 21–32. [CrossRef]
34. Lin, J.; Yu, W.; Yang, X.; Xu, G.; Zhao, W. On False Data Injection Attacks against Distributed Energy Routing in Smart Grid. In Proceedings of the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems, Beijing, China, 17–19 April 2012; pp. 183–192.
35. Ding, D.; Han, Q.L.; Xiang, Y.; Ge, X.; Zhang, X.M. A Survey on Security Control and Attack Detection for Industrial Cyber-Physical Systems. *Neurocomputing* **2018**, *275*, 1674–1683. [CrossRef]
36. Mahmoud, M.S.; Hamdan, M.M.; Baroudi, U.A. Modeling and control of Cyber-Physical Systems subject to cyber attacks: A survey of recent advances and challenges. *Neurocomputing* **2019**, *338*, 101–115. [CrossRef]
37. Zeng, Y.; Zhang, R. Active eavesdropping via spoofing relay attack. In Proceedings of the 2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Shanghai, China, 20–25 March 2016; pp. 2159–2163.
38. Jakobsson, M.; Wetzel, S.; Yener, B. Stealth attacks on ad-hoc wireless networks. In Proceedings of the 2003 IEEE 58th Vehicular Technology Conference, Orlando, FL, USA, 6–9 October 2003; Volume 3, pp. 2103–2111.
39. Ling, Z.; Liu, K.; Xu, Y.; Jin, Y.; Fu, X. An End-to-End View of IoT Security and Privacy. In Proceedings of the 2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–7.
40. Al-Alami, H.; Hadi, A.; Al-Bahadili, H. Vulnerability scanning of IoT devices in Jordan using Shodan. In Proceedings of the 2017 2nd International Conference on the Applications of Information Technology in Developing Renewable Energy Processes Systems (IT-DREPS), Piscataway, NJ, USA, 6–8 December 2017; pp. 1–6.
41. Kaushik, A.K.; Pilli, E.S.; Joshi, R.C. Network forensic system for port scanning attack. In Proceedings of the 2010 IEEE 2nd International Advance Computing Conference (IACC), Patiala, India, 19–20 February 2010; pp. 310–315.
42. Mitropoulos, D.; Spinellis, D. Fatal injection: A survey of modern code injection attack countermeasures. *PeerJ Comput. Sci.* **2017**, *3*, e136. [CrossRef]
43. Yan, R.; Xiao, X.; Hu, G.; Peng, S.; Jiang, Y. New deep learning method to detect code injection attacks on hybrid applications. *J. Syst. Softw.* **2018**, *137*, 67–77. [CrossRef]
44. Cazorla, L.; Alcaraz, C.; Lopez, J. Cyber Stealth Attacks in Critical Information Infrastructures. *IEEE Syst. J.* **2018**, *12*, 1778–1792. [CrossRef]
45. Douceur, J.R. The Sybil Attack. In *Peer-to-Peer Systems*; Springer: Berlin/Heidelberg, Germany, 2002; pp. 251–260.
46. Jan, M.A.; Nanda, P.; He, X.; Liu, R.P. A Sybil attack detection scheme for a forest wildfire monitoring application. *Future Gener. Comput. Syst.* **2018**, *80*, 613–626. [CrossRef]
47. Kaur, M.; Singh, A. Detection and Mitigation of Sinkhole Attack in Wireless Sensor Network. In Proceedings of the 2016 International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE), Ghaziabad, India, 22 September 2016; pp. 217–221.
48. Schirrmacher, N.B.; Ondrus, J.; Tan, F.T.C. *Towards a Response to Ransomware: Examining Digital Capabilities of the Wanna Cry Attack*; PACIS: Yokohama, Japan, 2018; p. 210.
49. Richardson, R.; North, M.M. Ransomware: Evolution, mitigation and prevention. *Int. Manag. Rev.* **2017**, *13*, 10.
50. Mohurle, S.; Patil, M. A brief study of Wannacry threat: Ransomware attack 2017. *Int. J. Adv. Res. Comput. Sci.* **2017**, *8*, 1938–1940.
51. CSRCN. Glossary-Virus Definition. 2018. Available online: https://csrc.nist.gov/glossary/term/virus (accessed on 23 September 2020).
52. CSRCN. Glossary-Spyware Definition. 2018. Available online: https://csrc.nist.gov/glossary/term/spyware (accessed on 23 September 2020).

53. CSRCN. Glossary-Cryptanalysis Definition. 2018. Available online: https://csrc.nist.gov/glossary/term/cryptanalysis (accessed on 23 September 2020).
54. CSRCN. Glossary-Side Channel Attack Definition. 2018. Available online: https://csrc.nist.gov/glossary/term/Side_Channel_Attack (accessed on 23 September 2020).
55. Deogirikar, J.; Vidhate, A. Security attacks in IoT: A survey. In Proceedings of the 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 10–11 February 2017; pp. 32–37.
56. Chelli, K. Security Issues in Wireless Sensor Networks: Attacks and Countermeasures. In Proceedings of the World Congress on Engineering, London, UK, 3–8 July 2015.
57. Inria. *Cybersecurity: Current Challenges and Inria's Research Directions*; Technical Report 3; Inria: Villeneuve-d'Ascq, France, 2019.
58. Goyal, P.; Parmar, V.; Rishi, R. Manet: Vulnerabilities, challenges, attacks, application. *IJCEM Int. J. Comput. Eng. Manag.* **2011**, *11*, 32–37.
59. Flauzac, O.; González, C.; Hachani, A.; Nolot, F. SDN Based Architecture for IoT and Improvement of the Security. In Proceedings of the 2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops, Gwangiu, Korea, 24–27 March 2015; pp. 688–693.
60. Shahzad, F.; Pasha, M.; Ahmad, A. A Survey of Active Attacks on Wireless Sensor Networks and their Countermeasures. *CoRR* **2017**, abs/1702.07136, 54–65.
61. Ahmad, K. Classification of Internet Security Attacks. In Proceedings of the 5th National Conference INDIACom-2011Bharti Vidyapeeth's Institute of Computer Applications and Management, New Dehli, India, 10–11 February 2011; pp. 973–7529.
62. Shanmuganathan, V.; Anand, T. A survey on gray hole attack in manet. *IRACST Int. J. Comput. Netw. Wirel. Commun. (IJCNWC)* **2012**, *2*, 647–650.
63. Apthorpe, N.; Reisman, D.; Sundaresan, S.; Narayanan, A.; Feamster, N. Spying on the smart home: Privacy attacks and defenses on encrypted IoT traffic. *arXiv* **2017**, arXiv:1708.05044.
64. Hernández Marcano, N.; Sørensen, C.; Cabrera G., J.; Wunderlich, S.; Lucani, D.; Fitzek, F. On Goodput and Energy Measurements of Network Coding Schemes in the Raspberry Pi. *Electronics* **2016**, *5*, 66. [CrossRef]
65. CSRCN. Glossary-Covert Channel Definition. 2018. Available online: https://csrc.nist.gov/glossary/term/covert_channel (accessed on 23 September 2020).
66. Krombholz, K.; Hobel, H.; Huber, M.; Weippl, E. Advanced social engineering attacks. *J. Inf. Secur. Appl.* **2015**, *22*, 113–122. [CrossRef]
67. Williams, E.J.; Hinds, J.; Joinson, A.N. Exploring susceptibility to phishing in the workplace. *Int. J. Hum.-Comput. Stud.* **2018**, *120*, 1–13. [CrossRef]
68. Alwan, Z.S.; Younis, M.F. Detection and prevention of SQL injection attack: A survey. *Int. J. Comput. Sci. Mob. Comput.* **2017**, *6*, 5–17.
69. Wang, C.; Zheng, X.; Chen, Y.; Yang, J. Locating Rogue Access Point Using Fine-Grained Channel Information. *IEEE Trans. Mob. Comput.* **2017**, *16*, 2560–2573. [CrossRef]
70. Gupta, A.; Jha, R.K. Security Threats of Wireless Networks: A Survey. In Proceedings of the International Conference on Computing, Communication Automation, Greater Noida, India, 15–16 May 2015; pp. 389–395.
71. Surman, G. Understanding Security Using the OSI Model. In *SANS Institute Reading Room*; Cyber Security Training, Certifications, Degrees and Resources: Boston, MA, USA, 2002.
72. Wenyuan, X.; Ma, K.; Trappe, W.; Yanyong Zhang, Y. Jamming sensor networks: Attack and defense strategies. *IEEE Netw.* **2006**, *20*, 41–47. [CrossRef]
73. Kolahi, S.S.; Treseangrat, K.; Sarrafpour, B. Analysis of UDP DDoS flood cyber attack and defense mechanisms on Web Server with Linux Ubuntu 13. In Proceedings of the 2015 International Conference on Communications, Signal Processing, and their Applications (ICCSPA'15), Piscataway, NJ, USA, 16–19 February2015; pp. 1–5.
74. Karchowdhury, S.; Sen, M. Survey on Attacks on Wireless Body Area Network. *Int. J. Comput. Intell. IoT Forthcom.* **2019**, 638–644. Available online: https://ssrn.com/abstract=3358378 (accessed on 2 August 2021).
75. CSRCN. Glossary-Cyber-Physical System(s). 2020. Available online: https://csrc.nist.gov/glossary/term/cyber_physical_systems (accessed on 25 September 2020).
76. Yang, C.; Shi, Z.; Zhang, H.; Wu, J.; Shi, X. Multiple Attacks Detection in Cyber-Physical Systems Using Random Finite Set Theory. *IEEE Trans. Cybern.* **2019**, *50*, 4066–4075. [CrossRef] [PubMed]
77. Karnouskos, S. Stuxnet worm impact on industrial cyber-physical system security. In Proceedings of the IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society, Melbourne, Australia, 7–10 November 2011; pp. 4490–4494.
78. Farwell, J.P.; Rohozinski, R. Stuxnet and the Future of Cyber War. *Survival* **2011**, *53*, 23–40. [CrossRef]
79. Zhang, X.; Han, Q.; Ge, X.; Ding, D.; Ding, L.; Yue, D.; Peng, C. Networked control systems: A survey of trends and techniques. *IEEE/CAA J. Autom. Sin.* **2020**, *7*, 1–17. [CrossRef]
80. Mousavinejad, E.; Yang, F.; Han, Q.; Vlacic, L. A Novel Cyber Attack Detection Method in Networked Control Systems. *IEEE Trans. Cybern.* **2018**, *48*, 3254–3264. [CrossRef] [PubMed]
81. Slay, J.; Miller, M. Lessons Learned from the Maroochy Water Breach. In *Critical Infrastructure Protection*; Springer: Boston, MA, USA, 2008; pp. 73–82.

82. Sahoo, S.; Mishra, S.; Peng, J.C.; Dragičević, T. A Stealth Cyber-Attack Detection Strategy for DC Microgrids. *IEEE Trans. Power Electron.* **2019**, *34*, 8162–8174. [CrossRef]
83. Kurt, M.N.; Ogundijo, O.; Li, C.; Wang, X. Online Cyber-Attack Detection in Smart Grid: A Reinforcement Learning Approach. *IEEE Trans. Smart Grid* **2019**, *10*, 5174–5185. [CrossRef]
84. Berghel, H. Wireless Infidelity I: War Driving. *Commun. ACM* **2004**, *47*, 21–26. [CrossRef]
85. Nurjahan, N.; Nizam, F.; Chaki, S.; Al Mamun, S.; Kaiser, M.S. Attack Detection and Prevention in the Cyber Physical System. In Proceedings of the 2016 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 7–9 January 2016; pp. 1–6.
86. Liang, G.; Weller, S.R.; Zhao, J.; Luo, F.; Dong, Z.Y. The 2015 Ukraine Blackout: Implications for False Data Injection Attacks. *IEEE Trans. Power Syst.* **2017**, *32*, 3317–3318. [CrossRef]
87. Elbez, G.; Keller, H.B.; Hagenmeyer, V. A New Classification of Attacks Against the Cyber-Physical Security of Smart Grids. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018; pp. 63:1–63:6.
88. Sakhnini, J.; Karimipour, H.; Dehghantanha, A. Smart Grid Cyber Attacks Detection Using Supervised Learning and Heuristic Feature Selection. In Proceedings of the 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Ontario, ON, Canada, 12–14 August 2019; pp. 108–112.
89. CSRCN. Glossary-Buffer Overflow. 2020. Available online: https://csrc.nist.gov/glossary/term/buffer_overflow (accessed on 10 September 2020).
90. Caballero, J.; Grieco, G.; Marron, M.; Nappa, A. Undangle: Early Detection of Dangling Pointers in Use-after-Free and Double-Free Vulnerabilities. In Proceedings of the 2012 International Symposium on Software Testing and Analysis. Association for Computing Machinery, Amsterdam, The Netherlands, 11–17 July 2012; pp. 133–143.
91. CSRCN. Glossary-Trojan Horse. 2020. Available online: https://csrc.nist.gov/glossary/term/trojan_horse (accessed on 10 September 2020).
92. Geer, D. Malicious bots threaten network security. *Computer* **2005**, *38*, 18–20. [CrossRef]
93. Nardone, R.; Rodríguez, R.J.; Marrone, S. Formal security assessment of Modbus protocol. In Proceedings of the 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, 5–7 July 2016; pp. 142–147.
94. IEEE Standards Association. Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3). 2012; pp. 1–821. Available online: https://ieeexplore.ieee.org/document/5518537 (accessed on 2 August 2021).
95. Akyildiz, I.F.; Su, W.; Sankarasubramaniam, Y.; Cayirci, E. Wireless sensor networks: A survey. *Comput. Netw.* **2002**, *38*, 393–422. [CrossRef]
96. Dey, N.; Ashour, A.S.; Shi, F.; Fong, S.J.; Sherratt, R.S. Developing residential wireless sensor networks for ECG healthcare monitoring. *IEEE Trans. Consum. Electron.* **2017**, *63*, 442–449. [CrossRef]
97. Geetha, A.; Sreenath, N. Byzantine Attacks and its Security Measures in Mobile Adhoc Networks. *Int. J. Comput. Commun. Instrum. Eng. (IJCCIE)* **2016**, *3*, 42–47.
98. Tamilselvan, L.; Sankaranarayanan, V. Prevention of Blackhole Attack in MANET. In Proceedings of the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007), Sydney, Australia, 27–30 August 2007; p. 21.
99. Mahajan, V.; Natu, M.; Sethi, A. Analysis of wormhole intrusion attacks in MANETS. In Proceedings of the MILCOM 2008–2008 IEEE Military Communications Conference, San Diego, CA, USA, 16–19 November 2008; pp. 1–7.
100. Khan, M.A.; Salah, A. IoT security: Review, blockchain solutions, and open challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
101. Wang, K.; Du, M.; Sun, Y.; Vinel, A.; Zhang, Y. Attack Detection and Distributed Forensics in Machine-to-Machine Networks. *IEEE Netw.* **2016**, *30*, 49–55. [CrossRef]
102. Anbalagan, G. NetSupport RAT Installed via Fake Update Notices. 2019. Available online: https://www.zscaler.com/blogs/research/netsupport-rat-installed-fake-update-notices, (accessed on 15 October 2020).
103. Gallais, A.; Hedli, T.; Loscri, V.; Mitton, N. Denial-of-Sleep Attacks against IoT Networks. In Proceedings of the 2019 6th International Conference on Control, Decision and Information Technologies (CoDIT), Paris, France, 23–26 August 2019; pp. 1025–1030.
104. Bhattasali, T.; Chaki, R.; Sanyal, S. Sleep Deprivation Attack Detection in Wireless Sensor Network. *CoRR* **2012**, abs/1203.0231, 19–25. [CrossRef]
105. Pongle, P.; Chavan, G. A survey: Attacks on RPL and 6LoWPAN in IoT. In Proceedings of the 2015 International Conference on Pervasive Computing (ICPC), Pune, India, 8–10 January 2015; pp. 1–6.
106. Jan, S.; Nguyen, C.D.; Briand, L.C. Automated and Effective Testing of Web Services for XML Injection Attacks. In Proceedings of the ISSTA 2016, Association for Computing Machinery, Saarbrücken, Germany, 18–20 July 2016; pp. 12–23.
107. Dhem, J.F.; Koeune, F.; Leroux, P.A.; Mestré, P.; Quisquater, J.J.; Willems, J.L. A Practical Implementation of the Timing Attack. In *Smart Card Research and Applications*; Springer: Berlin/Heidelberg, Germany, 2000; pp. 167–182.
108. Mohamad Noor, M.; Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294. [CrossRef]

109. ONF. OpenFlow Switch Specification. In *ONF Specification Version 1.5.1 (Protocol Version 0x06)*; Open Networking Foundation: Menlo Park, CA, USA, 2015; pp. 1–283.
110. Tayyaba, S.K.; Shah, M.A.; Khan, O.A.; Ahmed, A.W. Software Defined Network (SDN) Based Internet of Things (IoT): A Road Ahead. In Proceedings of the International Conference on Future Networks and Distributed Systems. Association for Computing Machinery, Cambridge, UK, 19–20 July 2017.
111. Ge, M.; Cho, J.H.; Ishfaq, B.; Kim, D.S. Modeling and Analysis of Integrated Proactive Defense Mechanisms for Internet-of-Things. In *Modeling and Design of Secure Internet of Things*; John Wiley & Sons, Ltd.: Chichester, UK, 2020; Chapter 10, pp. 217–247.
112. Xu, Y.; Liu, Y. DDoS attack detection under SDN context. In Proceedings of the IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications, San Francisco, CA, USA, 10–15 April 2016; pp. 1–9.
113. Mousavi, S.M.; St-Hilaire, M. Early detection of DDoS attacks against SDN controllers. In Proceedings of the 2015 International Conference on Computing, Networking and Communications (ICNC), Garden Grove, CA, USA, 16–19 February 2015; pp. 77–81.
114. Scott-Hayward, S.; O'Callaghan, G.; Sezer, S. SDN Security: A Survey. In Proceedings of the 2013 IEEE SDN for Future Networks and Services (SDN4FNS), Trento, Italy, 11–13 November2013; pp. 1–7.
115. Blial, O.; Ben Mamoun, M.; Benaini, R. An Overview on SDN Architectures with Multiple Controllers. *J. Comput. Netw. Commun.* **2016**, *2016*, 9396525. [CrossRef]
116. Mutlu, O.; Kim, J.S. RowHammer: A Retrospective. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.* **2020**, *39*, 1555–1571. [CrossRef]
117. Jay, J. Two Years after WannaCry, 2300 NHS Computers Are Still Running Windows XP. 2019. Available online: https://www.teiss.co.uk/nhs-computers-windows-xp/ (accessed on 28 October 2020).
118. Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. *Appl. Sci.* **2020**, *10*, 4102. [CrossRef]
119. Zhang, K.; Ni, J.; Yang, K.; Liang, X.; Ren, J.; Shen, X.S. Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Commun. Mag.* **2017**, *55*, 122–129. [CrossRef]
120. Alhalafi, N.; Veeraraghavan, P. Privacy and Security Challenges and Solutions in IOT: A review. *IOP Conf. Ser. Earth Environ. Sci.* **2019**, *322*, 012013. [CrossRef]
121. Ring, M.; Wunderlich, S.; Scheuring, D.; Landes, D.; Hotho, A. A Survey of Network-based Intrusion Detection Data Sets. *CoRR* **2019**, abs/1903.02460, 147–167. [CrossRef]
122. Junejo, K.N.; Goh, J. Behaviour-Based Attack Detection and Classification in Cyber Physical Systems Using Machine Learning. In Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security, Xi'an, China, 30 May 2016; pp. 34–43.
123. Creech, G.; Hu, J. Generation of a new IDS test dataset: Time to retire the KDD collection. In Proceedings of the 2013 IEEE Wireless Communications and Networking Conference (WCNC), Shanghai, China, 7–10 April 2013; pp. 4487–4492.
124. Creech, G.; Hu, J. A Semantic Approach to Host-Based Intrusion Detection Systems Using Contiguous and Discontiguous System Call Patterns. *IEEE Trans. Comput.* **2014**, *63*, 807–819. [CrossRef]
125. Creech, G. Developing a High-Accuracy Cross Platform Host-Based Intrusion Detection System Capable of Reliably Detecting Zero-Day Attacks. Ph.D. Thesis, University of New South Wales, Engineering & Information Technology, Sydnay, Australia, 2014.
126. The ADFA Intrusion Detection Datasets. 2013. Available online: https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-IDS-Datasets/ (accessed on 30 November 2020).
127. Kolias, C.; Kambourakis, G.; Stavrou, A.; Gritzalis, S. Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 184–208. [CrossRef]
128. AWID Dataset. 2015. Available online: http://icsdweb.aegean.gr/awid/index.html (accessed on 30 November 2020).
129. Santanna, J.J.; van Rijswijk-Deij, R.; Hofstede, R.; Sperotto, A.; Wierbosch, M.; Granville, L.Z.; Pras, A. Booters–An analysis of DDoS-as-a-service attacks. In Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, Canada, 18–21 May 2015; pp. 243–251.
130. Koroniotis, N.; Moustafa, N.; Sitnikova, E. andTurnbull, B. Towards the Development of Realistic Botnet Dataset in the Internet of Things for Network Forensic Analytics: Bot-IoT Dataset. *CoRR* **2018**, abs/1811.00701, 779–796.
131. Bot-IoT Dataset. 2018. Available online: https://research.unsw.edu.au/projects/bot-iot-dataset (accessed on 30 November 2020).
132. Biglar Beigi, E.; Hadian Jazi, H.; Stakhanova, N.; Ghorbani, A.A. Towards effective feature selection in machine learning-based botnet detection approaches. In Proceedings of the 2014 IEEE Conference on Communications and Network Security, San Francisco, CA, USA, 29–31 October 2014; pp. 247–255.
133. Botnet Dataset. 2014. Available online: https://www.unb.ca/cic/datasets/botnet.html (accessed on 30 November 2020).
134. The CAIDA "DDoS Attack 2007" Dataset. 2007. Available online: https://www.caida.org/data/passive/ddos-20070804_dataset.xml (accessed on 30 November 2020).
135. DDoS Evaluation Dataset (CIC-DDoS2019). 2019. Available online: https://www.unb.ca/cic/datasets/ddos-2019.html (accessed on 25 September 2020).
136. Sharafaldin, I.; Lashkari, A.H.; Hakak, S.; Ghorbani, A.A. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. In Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1–3 October2019; pp. 1–8.
137. Jazi, H.H.; Gonzalez, H.; Stakhanova, N.; Ghorbani, A.A. Detecting HTTP-based application layer DoS attacks on web servers in the presence of sampling. *Comput. Netw.* **2017**, *121*, 25–36. [CrossRef]

138. CIC DoS Dataset. 2017. Available online: https://www.unb.ca/cic/datasets/dos-dataset.html (accessed on 30 November 2020).
139. Sharafaldin, I.; Lashkari, A.H.; Ghorbani, A.A. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. In Proceedings of the International Conference on Information Systems Security and Privacy ICISSP, Funchal, Portugal, 22–24 January 2018; pp. 108–116.
140. Intrusion Detection Evaluation Dataset (CIC-IDS2017). 2017. Available online: https://www.unb.ca/cic/datasets/ids-2017.html (accessed on 30 November 2020).
141. Ring, M.; Wunderlich, S.; Grüdl, D.; Landes, D.; Hotho, A. Flow-based benchmark data sets for intrusion detection. In Proceedings of the 16th European Conference on Cyber Warfare and Security (ECCWS), ACPI, Dublin, Ireland, 29–30 June 2017; pp. 361–369.
142. CIDDS-Coburg Intrusion Detection Data Sets. 2017. Available online: https://www.hs-coburg.de/forschung/forschungsprojekte-oeffentlich/informationstechnologie/cidds-coburg-intrusion-detection-data-sets.html (accessed on 30 November 2020).
143. Ring, M.; Wunderlich, S.; Grüdl, D.; Landes, D.; Hotho, A. Creation of Flow-Based Data Sets for Intrusion Detection. *J. Inf. Warf.* **2017**, *16*, 40–53.
144. Sangster, B.; O'Connor, T.J.; Cook, T.; Fanelli, R.; Dean, E.; Adams, W.J.; Morrell, C.; Conti, G. Toward Instrumenting Network Warfare Competitions to Generate Labeled Datasets. In Proceedings of the 2nd Conference on Cyber Security Experimentation and Test, Montreal, QC, Canada, 10–14 August 2009; p. 9.
145. Point, U.S.M.A.W. CDX 2009 Dataset. 2009. Available online: https://www.westpoint.edu/centers-and-research/cyber-research-center/data-sets (accessed on 30 November 2020).
146. García, S.; Grill, M.; Stiborek, J.; Zunino, A. An empirical comparison of botnet detection methods. *Comput. Secur.* **2014**, *45*, 100–123. [CrossRef]
147. Lab, S. CTU-13 Dataset. 2009. Available online: https://www.stratosphereips.org/datasets-ctu13 (accessed on 30 November 2020).
148. Lippmann, R.; Haines, J.W.; Fried, D.J.; Korba, J.; Das, K. The 1999 DARPA off-line intrusion detection evaluation. *Comput. Netw.* **2000**, *34*, 579–595. [CrossRef]
149. DARPA. 1999. Available online: https://www.ll.mit.edu/r-d/datasets/1999-darpa-intrusion-detection-evaluation-dataset (accessed on 30 November 2020).
150. Perona, I.; Gurrutxaga, I.; Arbelaitz, O.; Martín, J.I.; Muguerza, J.; Pérez, J.M. Service-Independent Payload Analysis to Improve Intrusion Detection in Network Traffic. In Proceedings of the 7th Australasian Data Mining Conference, Glenelg, Australia, 27 November 2008; Volume 87, pp. 171–178.
151. Sahu, S.K.; Sarangi, S.; Jena, S.K. A detail analysis on intrusion detection datasets. In Proceedings of the 2014 IEEE International Advance Computing Conference (IACC), Gurgaon, Indian, 21–22 February 2014; pp. 1348–1353.
152. Gure KDD Cup. 2008. Available online: http://www.sc.ehu.es/acwaldap/gureKddcup/ (accessed on 30 November 2020).
153. Zuech, R.; Khoshgoftaar, T.; Seliya, N.; Najafabadi, M.M.; Kemp, C. A New Intrusion Detection Benchmarking System. In Proceedings of the FLAIRS Conference, Hollywood, FL, USA, 18–20 May 2015.
154. Shiravi, A.; Shiravi, H.; Tavallaee, M.; Ghorbani, A.A. Toward developing a systematic approach to generate benchmark datasets for intrusion detection. *Comput. Secur.* **2012**, *31*, 357–374. [CrossRef]
155. Intrusion Detection Evaluation Dataset (ISCXIDS2012). 2012. Available online: https://www.unb.ca/cic/datasets/ids.html (accessed on 30 November 2020).
156. Saad, S.; Traore, I.; Ghorbani, A.; Sayed, B.; Zhao, D.; Lu, W.; Felix, J.; Hakimian, P. Detecting P2P botnets through network behavior analysis and machine learning. In Proceedings of the 2011 Ninth Annual International Conference on Privacy, Security and Trust, Montreal, QC, Canada, 26–28 August2011; pp. 174–180.
157. Datasets. 2020. Available online: https://www.uvic.ca/engineering/ece/isot/datasets/ (accessed on 25 September 2020).
158. Tavallaee, M.; Bagheri, E.; Lu, W.; Ghorbani, A.A. A detailed analysis of the KDD CUP 99 data set. In Proceedings of the 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, ON, Canada, 8–10 July 2009; pp. 1–6.
159. Choudhary, S.; Kesswani, N. Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets using Deep Learning in IoT. *Procedia Comput. Sci.* **2020**, *167*, 1561–1573. [CrossRef]
160. KDD Cup 1999 Dataset. 1999. Available online: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (accessed on 30 November 2020).
161. Kent, A.D. Cybersecurity Data Sources for Dynamic Network Research. In *Dynamic Networks in Cybersecurity*; Imperial College Press: London, UK, 2015.
162. Kent 2016. 2016. Available online: https://csr.lanl.gov/data/cyber1/ (accessed on 30 November 2020).
163. Song, J.; Takakura, H.; Okabe, Y.; Eto, M.; Inoue, D.; Nakao, K. Statistical Analysis of Honeypot Data and Building of Kyoto 2006+ Dataset for NIDS Evaluation. In Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security, Association for Computing Machinery, Vienna, Austria, 17–20 August 2011; pp. 29–36.
164. Kyoto 2006+. 2016. Available online: https://www.takakura.com/Kyoto_data/ (accessed on 30 November 2020).
165. Pang, R.; Allman, M.; Bennett, M.; Lee, J.; Paxson, V.; Tierney, B. A First Look at Modern Enterprise Traffic. In Proceedings of the 5th ACM SIGCOMM Conference on Internet Measurement. USENIX Association, Berkeley, CA, USA, 19–21 October 2005; p. 2.
166. LBNL. 2004. Available online: http://icir.org/enterprise-tracing/Overview.html (accessed on 30 November 2020).

167. Beer, F.; Hofer, T.; Karimi, D.; Bühler, U. A new Attack Composition for Network Security. In *10. DFN-Forum Kommunikationstechnologien*; Gesellschaft für Informatik e.V.: Bonn, Germany, 2017; pp. 11–20.
168. NDSec-1. 2016. Available online: https://www2.hs-fulda.de/NDSec/NDSec-1/ (accessed on 30 November 2020).
169. Haider, W.; Hu, J.; Slay, J.; Turnbull, B.P.; Xie, Y. Generating realistic intrusion detection system dataset based on fuzzy qualitative modeling. *J. Netw. Comput. Appl.* **2017**, *87*, 185–192. [CrossRef]
170. NSL-KDD Dataset. 2019. Available online: https://www.unb.ca/cic/datasets/nsl.html (accessed on 25 September 2020).
171. Singh, R.; Kumar, H.; Singla, R.K. A Reference Dataset for Network Traffic Activity Based Intrusion Detection System. *Int. J. Comput. Commun. Control.* **2015**, *10*, 390–402. [CrossRef]
172. Sharma, R.; Singla, R.K.; Guleria, A. A New Labeled Flow-based DNS Dataset for Anomaly Detection: PUF Dataset. *Procedia Comput. Sci.* **2018**, *132*, 1458–1466. [CrossRef]
173. Wheelus, C.; Khoshgoftaar, T.M.; Zuech, R.; Najafabadi, M.M. A Session Based Approach for Aggregating Network Traffic Data–The SANTA Dataset. In Proceedings of the 2014 IEEE International Conference on Bioinformatics and Bioengineering, Boca Raton, FL, USA, 10–12 November 2014; pp. 369–378.
174. Vasudevan, A.R.; Harshini, E.; Selvakumar, S. SSENet-2011: A Network Intrusion Detection System dataset and its comparison with KDD CUP 99 dataset. In Proceedings of the 2011 Second Asian Himalayas International Conference on Internet (AH-ICI), Kathmundu, Nepal, 4–6 November 2011; pp. 1–5.
175. Bhattacharya, S.; Selvakumar, S. SSENet-2014 Dataset: A Dataset for Detection of Multiconnection Attacks. In Proceedings of the 2014 3rd International Conference on Eco-friendly Computing and Communication Systems, Mangalore, India, 18–21 December 2014; pp. 121–126.
176. Hofstede, R.; Hendriks, L.; Sperotto, A.; Pras, A. SSH Compromise Detection using NetFlow/IPFIX. *ACM Sigcomm Comput. Commun. Rev.* **2014**, *44*, 20–26. [CrossRef]
177. Hofstede, R. SSH Datasets. 2014. Available online: https://www.simpleweb.org/wiki/index.php/SSH_datasets (accessed on 30 October 2020).
178. Viegas, E.K.; Santin, A.O.; Oliveira, L.S. Toward a reliable anomaly-based intrusion detection in real-world environments. *Comput. Netw.* **2017**, *127*, 200–216. [CrossRef]
179. Laboratory, S.P. TRAbID-Datasets. 2019. Available online: https://secplab.ppgia.pucpr.br/?q=trabid (accessed on 30 October 2020).
180. Bhuyan, M.H.; Bhattacharyya, D.; Kalita, J. Towards Generating Real-life Datasets for Network Intrusion Detection. *Int. J. Netw. Secur.* **2015**, *17*, 683–701.
181. Sperotto, A.; Sadre, R.; van Vliet, D.F.; Pras, A. A Labeled Data Set For Flow-based Intrusion Detection. In Proceedings of the 9th IEEE International Workshop on IP Operations and Management, IPOM 2009, Venice, Italy, 29–30 October 2009; Springer: Berlin, Germany, 2009; Volume 5843, pp. 39–50.
182. Laboratory, S.P. Twente-Datasets. 2012. Available online: https://www.simpleweb.org/wiki/index.php/Labeled_Dataset_for_Intrusion_Detection (accessed on 30 October 2020).
183. Maciá-Fernández, G.; Camacho, J.; Magán-Carrión, R.; García-Teodoro, P.; Therón, R. UGR'16: A new dataset for the evaluation of cyclostationarity-based network IDSs. *Comput. Secur.* **2018**, *73*, 411–424. [CrossRef]
184. UGR'16-Datasets. 2016. Available online: https://nesg.ugr.es/nesg-ugr16/ (accessed on 30 October 2020).
185. Gringoli, F.; Salgarelli, L.; Dusi, M.; Cascarano, N.; Risso, F.; Claffy, K.C. GT: Picking up the Truth from the Ground for Internet Traffic. *SIGCOMM Comput. Commun. Rev.* **2009**, *39*, 12–18. [CrossRef]
186. UNIBS-2009-Datasets. 2016. Available online: http://netweb.ing.unibs.it/~ntw/tools/traces/ (accessed on 30 October 2020).
187. Turcotte, M.J.M.; Kent, A.D.; Hash, C. Unified Host and Network Data Set. In *Data Science for Cyber-Security*; World Scientific: Singapore, 2018; Chapter 1, pp. 1–22.
188. Unified Host and Network Data Set. 2017. Available online: https://csr.lanl.gov/data/2017/ (accessed on 30 October 2020).
189. Moustafa, N.; Slay, J. UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In Proceedings of the 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, Australia, 10–12 November 2015; pp. 1–6.
190. UNSW-NB15 Dataset. 2015. Available online: https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/ (accessed on 30 October 2020).