IoT Critical Infrastructure security

Subjects: Others
Contributor: Nathalie Mitton

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.

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

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.

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.

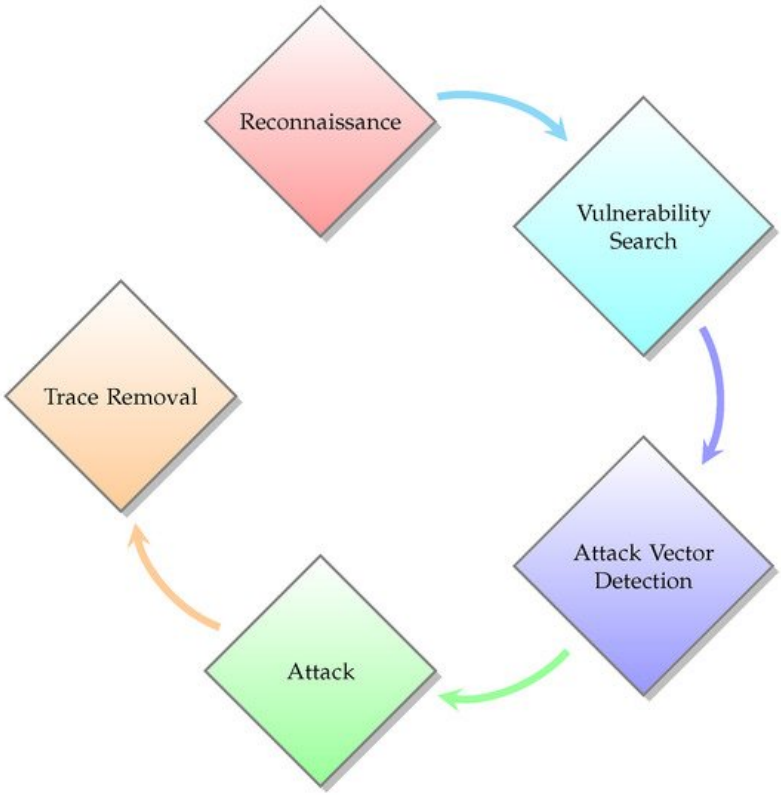

Figure 1. Cyber Attack Steps.

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].

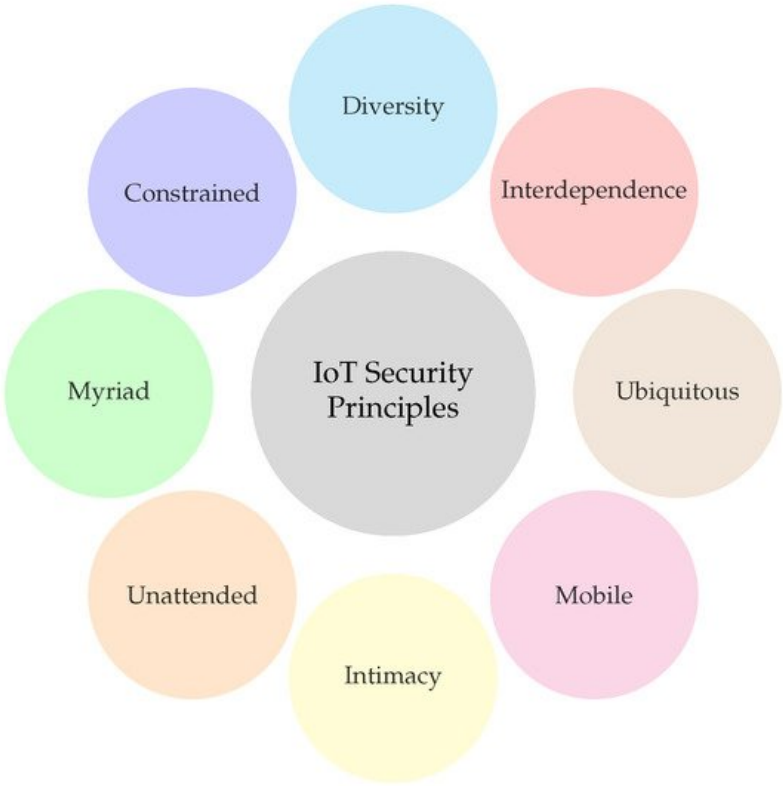

Figure 2. IoT Security Principles.

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.

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.
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.
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.
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.
