Security Challenges for Modern Data Centers with IoT: A Preliminary Study

Zhen Zeng, Chun-Jen Chung, Liguang Xie
Futurewei Technologies
Bellevue, WA, USA
{zzeng, cchung, lxie}@futurewei.com

ABSTRACT

The wide deployment of internet of things (IoT) devices makes a profound impact on the data center industry from various perspectives, varying from infrastructure operation, resource management, to end users. This is a double-edged sword – it enables ubiquitous resource monitoring and intelligent management therefore significantly enhances the efficiency of daily operation while introducing new security issues for modern data centers. The emerging security challenges are not only related to detecting new IoT attacks or vulnerabilities but also including the implementations of cybersecurity protection mechanisms (e.g., intrusion detection system, vulnerability management system) to enhance data center security. As the new security challenges with IoT have not been thoroughly explored in the literature, this paper provides a survey on the most recent IoT security issues regarding modern data centers by highlighting IoT attacks and the trend of newly discovered vulnerabilities. We find that vulnerabilities related to data center management system have increased significantly since 2019. Compared to the total amount in 2018 (with 25 vulnerabilities), the number of data center management system vulnerabilities almost increased by a factor of four times (with 98 vulnerabilities) in 2020. This paper also introduces the existing cybersecurity tools and discusses the associated challenges and research issues for enhancing data center security.

CCS CONCEPTS

• **Security and privacy → Systems security**; • **Information systems → Data centers**; • **Computer systems organization → Embedded and cyber-physical systems**;

KEYWORDS

Internet of Things, Data Center, Security

ACM Reference Format:
Zhen Zeng, Chun-Jen Chung, Liguang Xie. 2022. Security Challenges for Modern Data Centers with IoT: A Preliminary Study. In *Companion Proceedings of the Web Conference 2022 (WWW '22 Companion), April 25–29, 2022, Virtual Event, Lyon, France.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3487553.3524857

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
WWW '22 Companion, April 25–29, 2022, Virtual Event, Lyon, France
© 2022 Association for Computing Machinery.
ACM ISBN 978-1-4503-9130-6/22/04…$15.00
https://doi.org/10.1145/3487553.3524857

1 INTRODUCTION

In recent years, large-scale deployment of Internet of Things (IoT) devices has become an inevitable trend due to the advancement of communication and manufacturing technologies, significant cost reduction, and a rich set of business scenarios in consumer and industrial sectors [31], with the number of IoT devices doubling every five years [32]. Among this trend, IoT devices that connect to the enterprise infrastructure are expected to reach more than 15 billion by 2029 [32]. For the data center industry, IoT devices potentially affect the development of technology and market (such as, target customers, technology providers, and sales and marketing models [31]) in modern data centers, which are more intelligent and efficient compared to traditional data centers [66]. It is worth mentioning that such effects are transformative [31–33], which result in considerable changes in various perspectives from the infrastructure design and operation of data centers (e.g., data center network, storage management, server technologies, power supply systems, etc.) to end users (e.g., consumer privacy) [14, 32, 33]. For example, IoT sensors support the "smart" operation on energy management in a data center, fog computing is developed to connect the communication between IoT devices and the cloud data centers as a middle layer, and the rate and volume of data generated by IoT devices contribute to the formation of mega data centers [33].

Along with such changes, one of the major concerns is security [6, 24, 25, 33, 68]. Kaspersky reports that there are 1.51 billion breaches of IoT devices detected world-wide via the"honeypots" in the first half-year of 2021. Such IoT attacks are increased to twice what was in 2020 [61]. Regarding data centers, the role of security in a data center is critical [33]. Once a data center is taken down by attacks, it might lead to tremendous damage to data storage, running services, reputation, and revenue [16]. The recent study also reveals emerging threats of using IoTs are identified in cloud and edge data centers [60]. For example, the cross-vendor/cross-cloud access delegation mechanisms of IoT cloud and the complicated interactions among IoT devices, IoT cloud, and mobile apps might allow attackers to gain unauthorized access to a user's cloud credentials, and then rise security risk to cloud providers [4, 87]. Compared to traditional malware, IoT malware is more difficult to be detected by signature-based detection [84]. However, the security challenges related to IoT devices in modern data centers have not been thoroughly explored.

This paper provides a survey on the most recent security issues related to IoT in modern data centers by reviewing publications in the top security conferences since 2018 in Section 3.1 (e.g., IEEE Symposium on Security and Privacy (S & P) [38], ACM Conference on Computer and Communications Security (CCS) [1], USENIX Security Symposium (Security) [75], and Network and Distributed

System Security Symposium (NDSS) [55]), and investigating the trends of emerging vulnerabilities associated with IoT and data centers (discussed in Section 3.2). This paper also highlights the existing cybersecurity tools and the associated challenges and research issues in Section 4.

This paper is organized as follows. In Section 2, we introduce the background of modern data centers, IoT basics, and how IoT deployment affects modern data centers. We summarize the recent IoT security issues in Section 3 and discuss security challenges and issues for enhancing security in modern data centers in Section 4. In Section 5, we conclude this paper.

2 BACKGROUND

In this section, we briefly describe the fundamentals of IoT and modern data centers including the key components of data centers, and illustrate how IoT affects modern data centers through an example of modern data center deployments.

2.1 Basics of Modern Data Centers & IoT

Modern data centers refer to various types of data centers that are designed or operated in a way that is smarter, more intelligent, and efficient on deployment, maintenance, or applications, compared to traditional data centers [66]. The examples of modern data centers contain, but are not limited to, green data centers [46, 47], edge data centers [59, 62, 83], and so on. The infrastructure of a modern data center is complex, where multiple components interact either sequentially or simultaneously. To host services and store data for an enterprise, a data center contains a collection of key components as the server, storage, network, power, and cooling infrastructures [8, 10, 26, 46].

- Server: typically, servers are mounted within a rack and are interconnected by switches at the cluster level or data center level [8]. Customers' applications are hosted by the clusters of hundreds or thousands of servers [10]. Ensuring server availability is one of the key performances in the operation of data centers [26].
- Storage: traditionally, disks and flash SSDs are used as the building blocks of storage systems. The storage system manages storage devices in the data center and provides application programming interfaces (APIs) for application developers. Sophisticated distributed storage systems usually need to make several trade-offs based on various requirements when considering the aggregate capacity, bandwidth, and latency [8]. The massive data growth (e.g., in social media, personal electrical devices, etc.) within recent years predominantly affects the design and operation of data center storage infrastructure.
- Network: is a critical infrastructure that interconnects the server and storage infrastructures [26], and can support various protocols for the communication among devices. As network technology developed, the network infrastructure becomes a complex combination of various network devices (e.g., routers, switches, interfaces, etc. [8]), network architectures (e.g., software defined networking, switch/server-centric architectures, hybrid architectures, etc. [86]), and networking technologies (e.g., network virtualization, virtual desktop interface, cloud gaming, etc. [10]). The design of a data center network could influence the performance of data centers (e.g., latency, fault tolerance, routing efficiency, etc.) by interacting with other data center features (e.g., data center topology, traffic characteristics, etc.) [26, 86].
- Power: is one of the main data center components and is highly related to the data center's cost and availability [26]. The power infrastructure combines the holistic and hierarchical power delivery design to support the enormous power consumption in data centers. In the holistic design, power is distributed based on functional roles in a data center, while in the hierarchical design, power is distributed based on the hierarchy of buildings and physical data center rows [8]. Power disruption is one of the main reasons for the failures of most data centers [29].
- Cooling: is one of the important infrastructures regarding the reliability of electronic components in a data center. Running a data center in the situation that is above the common operating temperature will cause both the data center and the electronic components' performance degrade (e.g., by increasing every 2 °C, a data center might suffer performance degradation of 10%) [26].

IoT devices refer to wearable devices (e.g., smartwatches, glasses, health monitors, etc.), smart appliances (e.g., smart locks, sensors for temperature, gas, light, etc.), and smart devices for industrial automation and logistics (e.g., autonomous vehicles, drones, etc.) [70]. IoT devices can support the connectivity and data transfer from end users to data centers through wireless telecommunication technologies, such as machine-to-machine communication, context-aware computing, and radio-frequency identification (RFID) [7, 70]. To connect different components over the network, researchers propose different IoT architectures based on the application domains. There are two predominant IoT architectures as the three-layer architecture and the four-layer service-oriented architecture. The three-layer architectural model has the sensor layer (a.k.a., perception layer), network layer, and application layer [45]:

- Sensor layer: interacts with physical smart devices (e.g., RFID, sensors, etc.), and processes the data collected from all IoT devices in the network to the upper layer through layer interfaces.
- Network layer: receives the processed data from sensor layer and determines the routes of data transmission. The network layer integrates various devices (e.g., IoT hub, switching, gateway, etc.) and various communication technologies (e.g., Ethernet, Bluetooth, Wi-Fi, cellular, etc.), and is the most important layer in the IoT architecture. In some cases, the network layer also provides the data services, such as data aggregation, data computing, and so on.
- Application layer: provides services or operations (e.g., storage service, data analysis service, data mining services, etc.) based on the transmitted data from the network layer.

A service-oriented architecture (SoA) is proposed to connect different services components of an application via interfaces and protocols [20, 45]. By designing the workflow of coordinated services, the SoA-based architecture enables the reuse of software and

hardware components and extracts out the data services provided in the network and application layers in the three-layer architecture. To ensure the communications between devices and cooperative event processing among them, a service layer could simplify the management and interconnection of these IoT devices [20].

2.2 When Data Center Meets with IoT

We illustrate modern data centers with IoT in Figure 1 and explain how IoT devices shape data center deployments. Generally, based on the device geolocation, there are two typical working scenarios: 1) IoT devices work as the components of a data center infrastructure to support the operation. For example, using IoT sensors to support smart temperature control, providing real-time insights of facilities (e.g., using temperature sensors to monitor heat generation); and 2) IoT devices work as the endpoints to generate data (e.g., IoT sensors, health monitors, drones, etc.).

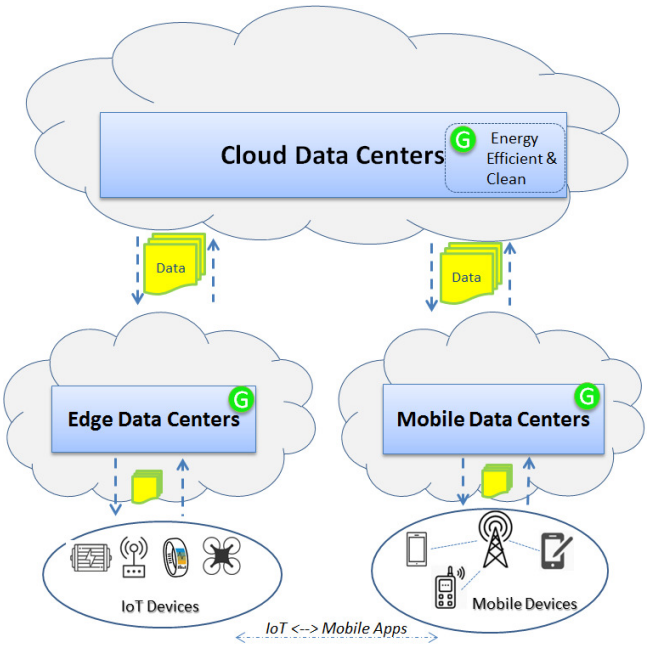

Figure 1: An Example of Data Center Deployments

Figure 1 shows an example of data center deployments, including cloud data center, edge data center, mobile data center, and green data center. The cloud data center (a.k.a., core data center) is used to house and maintain the data center facilities to provide cloud service. Energy management is one of the critical challenges for cloud data centers, which increase by about 20% to 25% every year [33]. To improve the energy efficiency, as shown in Figure 1, the design of "green" (e.g., using energy-efficient equipment, clean energy, etc.) is integrated into the practices of current modern data centers. Green data center aims to reduce the energy consumption of data centers while guaranteeing performance at the same time [46, 47]. Among a breakdown analysis of energy consumption for the key components of a data center, the cooling infrastructure consumes about 50% of the data center energy [22]. IoT devices well support the energy-efficiency improvements of green data centers by 1) working as "green" equipment (e.g., smart IoT sensors that can selectively sense) in the design and construction of data centers; and 2) supporting the energy-efficiency in the daily operation [10, 42], such as IoT sensors that collect a broad range of information to adjust environmental temperatures for smart heating and cooling system [47], detecting the water leakage (e.g., rope sensors, spot leak sensors) [9], and so on.

The edge data center refers to the data center that works as an intermediate layer between IoT devices of end users and core data center and usually has limited storage and processing capabilities [60]. Edge data centers better support end users to access applications or services nearby compared to the traditional centralized data center [74, 86]. IoT devices work as the end points to generate data, which usually are high volume. This kind of IoT data has a fast data rate and unreliable value since such data are uploaded from a wide range of real-world IoT applications [82]. To send these IoT data to a data center, the data path usually contains different gateways and networking devices. For example, for an edge data center, the IoT sensor data is aggregated on the edge data center and then transmitted to the core data center either in a single hop or multiple hops [60].

The mobile data center is the intermediate layer that supports the data transmission between mobile users and data centers [71]. In practice, end users interact with IoT devices by using mobile apps via Bluetooth communications, which will also lead to some security issues to a data center, such as, attackers can compromise an IoT device from the companion mobile app, and gain unauthorized access to cloud resources with the authentication of such IoT [88].

3 RECENT IOT SECURITY ISSUES FOR MODERN DATA CENTERS

As we discuss in Section 2, IoT has been widely implemented in the modern data center. A recent study reveals that IoT security becomes more and more critical and the attacks against IoT devices increased dramatically since 2017 [70]. In this section, we review the existing study on IoT security in the top security conferences and summarize the IoT attacks discussed in these publications in Section 3.1. Specifically, we associate the IoT attacks to data centers based on the attack targets and explain how attackers might utilize IoT devices to damage a data center. In Section 3.2, we investigate the trend of newly discovered vulnerabilities related to IoT and data centers.

3.1 Recent IoT Attacks

The IoT attacks usually are stealthy, some of them even do not hack or interact with the victim directly, e.g., stealing the sensing data (i.e., TEMPEST attack). We summarize the IoT attacks that have been explored in top security conferences in recent years. These IoT attacks either have new attack features or have new attack methods compared to traditional cybersecurity attacks. We summarize the potential consequences of these IoT attacks if applied to data centers in Table 1, and further illustrate these IoT attacks as follows. As shown in Table 1, there are six recent IoT attacks discussed in this section, where three of them might directly lead to authentication or data leakage (e.g., brute-force attack, spoofing attack, and TEMPEST

Table 1: The Consequence of IoT Attacks on Data Centers

IoT Attacks	Consequence
Brute-force Attack	Authentication leakage, unauthorized access to cloud
Spoofing Attack	Authentication leakage, unauthorized access to cloud
TEMPEST Attack	Data leakage
DoS Attack	Disrupt service to legitimate cloud users
MadIoT Attack	Disrupt the power grid of a data center
Energy Consumption Attack	Exhaust the battery-powered IoT devices of a data center

attack), and the rest might disrupt the services related to a data center (e.g., DoS attack, MadIoT attack, and Energy Consumption attack).

Brute-force attack: attackers attempt to guess the password or authentications by systematically checking all possible passwords until successfully logging in to an account [27]. A successful brute-force attack usually can enable the persistent access of the victim system to attackers. Regarding the security of the cloud and IoT appliances, the recent study shows that the leaked SSH keys of IoT appliances have been used by attackers to conduct SSH brute-force attacks via the major cloud providers (e.g., Google, Charter Communications) [79].

Spoofing attack: refers to the attack that an attacker impersonates a legitimate user or a trusted source (e.g., IP address, domain name system (DNS) server, address resolution protocol (ARP) service, etc.) to the victims. By taking advantage of this trusted relationship with the victim, attackers can compromise the victim and lead to serious consequences, such as stealing sensitive data, spreading malware, bypassing access control, launching a DoS attack, a man-in-the-middle attack, and so on [63]. Spoofing attack has been reported recently in IoT attacks, especially for the devices or systems that are "smart" to perform autonomous actions without centralized control, where sensing and actuation are key components to support operation [44]. Attackers conduct spoofing attacks on IoT sensors by exploiting the sensors in the autonomous system. Such attacks can compromise the integrity of data by injecting malicious data or generating malicious network packets [36, 44].

TEMPEST attack: refers to the attack via listening to IoT devices remotely without actually hacking or interacting with the victim system directly. Data leakage might happen on, but is not limited to, unintentional radio, electrical signals, sounds, and vibrations [80]. As IoT device design developed, the IoT integrated design brings new security issues related to the TEMPSET attack. For example, to minimize the size of IoT devices, multiple components (e.g., digital, analog, power circuits, etc.) are integrated into a single chipset. A new TEMPEST attack has been detected on such a mixed-signal system on chip (MSoC). A typical power circuit of the switching regulator is integrated into the MSoC. According to the recent study [12], the TEMPEST attack has been detected on this system, where attackers can steal the original plain audio information remotely by exploiting the unintentional electromagnetic (EM) radiations. This attack is due to the switching noise from the integrated switching regulator, where an audio signal is coupled with such noise and makes the leaked EM signals dense, wideband and static. In this situation, attackers have a longer attack range and are more robust to interferences [12].

Denial of service (DoS) attack: refers to the attack that attackers aim to temporarily or indefinitely prevent the legitimate use of a service by flooding the target with a large amount of traffic or requests (e.g., SYN flood, ACK flood, etc.). When the incoming flooding traffic/requests come from various sources to the targeted victim, it is called a distributed denial of service (DDoS) attack [78]. In the DDoS attack, attackers usually initiate flooding to the target from machines via a botnet. The Mirai botnet is one recently identified botnet that primarily targets embedded and IoT devices (such as IP cameras, routers, printers, etc.) in 2016. This botnet can infect around 65k IoT devices in 20 hours when reaching the population of 200k-300k infections [6]. The Hajime botnet is another recently identified IoT botnet, which contains over 95k active bots [35].

Manipulation of demand via IoT (MadIoT) attack: refers to "*attacks that allow an adversary to disrupt the power grid's normal operation by manipulating the total power demand using compromised IoT devices [68].*" It is a new class of attack that leverages the IoT botnet of high wattage devices (e.g., air conditioners, heaters, etc.) to launch large-scale coordinated attacks on the power grid [68]. Researchers reveal that the essential infrastructure of the power grid can be disrupted by attackers via utilizing compromised IoT devices [68].

Energy consumption attack: refers to the attack that aims to exhaust the energy of the battery-powered IoT devices [54]. Because IoT devices usually have limited battery power, this type of attack can force the end devices (e.g., sensors) to consume battery power and then cause energy exhaustion [43], especially, in the working scenario (e.g., Long-Range Wide Area Network) that requires low energy consumption on the end devices [54]. The recent study show that an energy consumption attack can be accomplished by flooding the target (e.g., via the DoS attack) to exhaust the victim IoT devices [54, 69].

3.2 Emerging Trend of NVD Vulnerabilities

The ISO/IEC 27000:2018 standard defines a vulnerability as "*a weakness of an asset or control that can be exploited by one or more threats*" [41]. Vulnerabilities can be exploited by attackers to deliver a successful attack. In practice, a vulnerability can be registered by MITRE into the Common Vulnerability and Exposures (CVE) system [50]. Each vulnerability is assigned a Common Vulnerability Scoring System (CVSS) score to indicate its potential severity level to an organization [72]. In this Section, we investigate vulnerabilities in the national vulnerability database (NVD) [73] and summarize the trend of newly discovered vulnerabilities that are related to IoT and data centers as Figures 2 and 3.

We first search the IoT-related vulnerabilities by using the keyword of "IoT" and "internet of things" in the NVD [50], leading to 999 vulnerabilities related to IoT in total until February 2022. Figure 2 shows the count of new NVD vulnerabilities that are related to IoT in the recent five years from 2017 to 2021. It indicates that IoT-related vulnerabilities increases at a high rate (in about 100-200% increment) in 2017-2019 and reaches the peak amount of 366

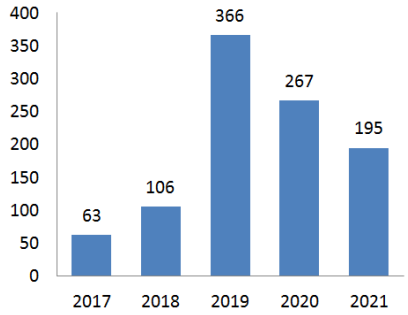

Figure 2: The Count of NVD Vulnerabilities Related to IoT in 2017-2021

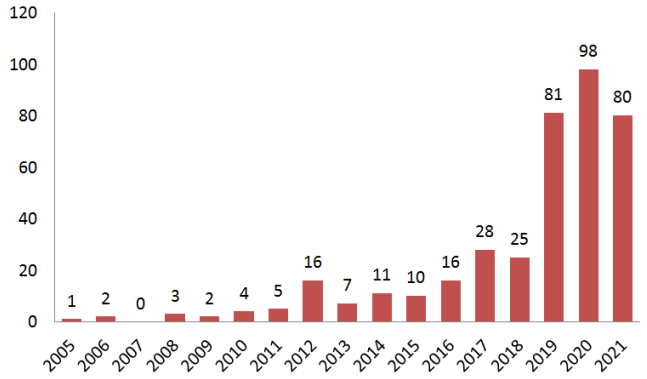

Figure 3: The Count of NVD Vulnerabilities Related to Data Center Management System in 2005-2021

vulnerabilities in 2019. This summary provides a quick overview of vulnerabilities that directly highlight IoTs in the vulnerability descriptions.

There remain a large number of vulnerabilities that might be not covered in this summary and can affect IoT security. For example, Bluetooth Low Energy (BLE) is widely used in IoT devices and is vulnerable at the link layer during broadcasting, pairing, and message transmission [76, 88]. Attackers can precisely fingerprint a BLE device with static UUIDs from the companion mobile app [88]. The recent study also successfully demonstrates the identity tracking, spoofing, and eavesdropping attacks on BLE, and highlights the related security issues [76]. According to the recent record in NVD [73], Bluetooth-related vulnerabilities could lead to system crashes, information leakage, or privilege escalation on the victim system. 532 vulnerabilities are associated with Bluetooth until February 2022 [51], which might cause potential damage to the IoT security.

We also investigate vulnerabilities that directly affect the security of data centers. By searching vulnerability in NVD with the keywords of "data center", there are 390 vulnerabilities related to the data center management system until 2021 [52]. These vulnerabilities are associated with some popular data center management tools, such as Cisco Prime Data Center Network Manager (CVE-2017-6639, CVE-2018-0144, CVE-2018-0258, etc.), Atlassian Jira Server and Data Center (CVE-2021-43953, CVE-2021-39113, etc.), Intel(R) Data Center Manager SDK (CVE-2018-3703, CVE-2019-0106, etc.), and so on. Figure 3 shows the amount of NVD vulnerabilities relevant to data centers in each year ranging from 2005 to 2021, and clearly indicates that such vulnerabilities have increased significantly since 2019. Compared to the total amount in 2018 (with 25 vulnerabilities), the number of data center vulnerabilities almost increased by a factor of four times (with 98 vulnerabilities) in 2020. How to manage such vulnerabilities and ensure the security in a data center becomes more and more critical and challenging.

4 ENHANCING SECURITY IN MODERN DATA CENTER

In this section, we first introduce some popular cybersecurity approaches on intrusion detection, vulnerability management, and network security situational awareness, and then illustrate the challenges and research issues for enhancing security in modern data centers from the perspectives of attack detection, vulnerability management, and system recovery.

4.1 Existing Cybersecurity Tools

Intrusion Detection System. The intrusion detection system (IDS) aims to offer alarm on threats and provides the corrective steps in the network [11]. According to the design of the analysis model, IDS can be categorized as signature-based IDS and anomaly-based IDS. The signature-based IDS pre-defines patterns or signatures by analyzing the discovered attacks. This approach requires a signature database that is corresponding to the known attacks and has limitations on detecting new attacks that have never been encountered before. The anomaly-based IDS generates an alarm for observation when the difference between the observed behavior and the expected one falls below a given threshold [11]. The recent anomaly-based IDS well adopts AI technologies into system design, such as deep learning, logical reasoning, natural language processing, etc. to efficiently and effectively analyze network security status. For example, [24] proposes anomaly-based IDS algorithms for IoT-empowered DDoS attacks, [28] integrates the semantic information into anomaly detection model to improve the performance of IoT attack detection, and [18] develops a signature-based IDS for IoT, which enable to run on resource-constrained devices.

Vulnerability Management System. In practice, vulnerability management contains three main steps. First, defenders identify vulnerabilities in the system (e.g., by using vulnerability scanning tools, such as Nessus [77], Nmap [48], etc.), and they assess and prioritize vulnerabilities according to the assessed risk levels. Then, they remediate the system by mitigating or removing identified vulnerabilities based on their assessed risk rankings [23]. By ranking the risk of vulnerability from high to low, vulnerabilities that are at the top will be recommended for remediation first. Traditionally, vulnerabilities' risks are identified by the CVSS score [72]. The widely used CVSSv2 scoring system was launched in 2007 by defining the severity level of a vulnerability as Low (0-3.9), Medium (4-6.9), and High (7-10). However, the CVSS score does not indicate the risk of vulnerability well in real attacks [2], new vulnerability risk assessment methods are proposed to assess vulnerability risk by

integrating the attacker model [3, 85], early exploit detection [64], or emerging threats in the online hacker community [65].

Network Security Situational Awareness. Network security situational awareness refers to the perception, comprehension, and projection of a network system security [37]. Using the attack graph as an example, it predicts the attacker's next steps or the ultimate goal of attack by traversing on a graph to identify a successful attack path in a network system [58]. Such attack paths contain a set of aspects of the network, such as vulnerabilities, network connectivity and configuration, current conditions and exploits of network states, etc., and the relationship among all of them. An attack graph consists of nodes and edges, where a node represents states (such as host, privilege, exploit, vulnerability, etc.) and an edge represents a directed transition from pre-condition to post-condition when executing an event. The network security situational awareness usually contains attack projection, attack intention recognition, attack prediction, and security situation forecasting within a range of time and space [37]. There are some tools for analyzing attacker paths that are developed based on attack graph model, such as MulVal [58], NetSPA [39], NICE [13], and so on.

4.2 Security Challenges and Research Issues for Data Centers

We focus on the challenges and research issues for enhancing security in modern data centers with IoT from the perspectives of attack detection, vulnerability management, and system recovery.

Challenge 1: Attacks for data centers become more complicated. The attacks discussed in Section 3 can be conducted individually or cooperatively as a set of attacks for sophisticated levels of cyber attack, e.g., the advance persistent threat (APT) attack [57]. Although the APT attacks are not the main attacks on a data center currently [67], Dutch data centers have been compromised by APT attacks in 2021 [21]. APT targets to steal important information or cause damage to critical systems, such as financial institutions, military defense, aerospace, healthcare, and so on. A typical APT attack contains several stages as [49]:

(1) *Reconnaissance:* gather information about the target;
(2) *Delivery:* deliver exploits to the target;
(3) *Initial Intrusion:* get first unauthorized access to the target;
(4) *Command and Control:* control compromised hosts;
(5) *Lateral Movement:* move inside network and expand control;
(6) *Data Exfiltration:* steal sensitive data.

The challenge of APT attack investigation is to identify the stealthy attack vectors that are hidden among the normal activities. In the real-world scenario, the attack model of APT usually has a minimal footprint to perform malicious activities [5]. In the APT attack, attackers can slowly penetrate a system. The stealthy feature of APT attacks might not be captured by a time-based intrusion detection system since the initial attack that happened a long time ago was forgotten [34, 49]. Additionally, such malicious events are at an extremely small portion (e.g., 0.5% of the dataset [56]) compared to normal events, which makes the APT attack very difficult to be detected. Therefore, how to secure the data center to defend against this kind of advanced attack is one of the emerging challenges.

Challenge 2: Effectively managing vulnerabilities in a data center. As discussed in Section 3.2, both IoT devices and data center management tools are vulnerable. One product might become vulnerable after being released on the market when attackers find new security bugs or hacking methods. Thus, how to efficiently and effectively handle these vulnerable components is challenging. For example, only for data center management and monitoring products, there are more than 20,000 vulnerable web instances reported recently [19]. Attackers could leverage the unpatched vulnerabilities to harm critical assets of data centers. Therefore, an efficient and effective vulnerability management solution is essential for securing a data center. For example, Microsoft secures the data centers by running a Threat, Vulnerability, and Risk Assessment program [15]. Gartner [53] recommends that an effective vulnerability management framework should align vulnerability management to organization's needs and requirements, and prioritize vulnerabilities based on its risk attributes. For the selection of remediation solutions, the compensating controls and automate vulnerability analysis could better support the effective vulnerability management in practices. Some existing risk-based vulnerability management systems (e.g., Tenable [17]) have utilized machine learning techniques to correlate asset criticality, vulnerability severity, and threat actor activity, and helps cyber administrators focus on the relatively few vulnerabilities that pose the most risk to an organization. However, cloud computing techniques and the large-scale deployments of IoT devices in data centers might bring challenges to risk-based vulnerability management. For example, some newly created business applications are outside of IT visibility and traditional enforcement. The cloud-based and highly modular architecture makes it much more difficult to control digital assets that are outside of a data center [30].

Challenge 3: Recovering the compromised IoT devices in a data center. IoT devices are widely deployed in the modern data center industry and are also subject to attack and compromise. Attackers could gain unauthorized access to a user's cloud via compromising the connected IoT devices. By gaining unauthorized access to the cloud, the attacker might lead to a more serious security risk to the cloud provider [4, 87]. Thus, recovering the large IoT devices from root compromise is critical for the security of a data center. However, the traditional data center management solutions (e.g., the Intelligent Platform Management Interface (IPMI) [40]) might not efficiently support the existing IoT hardware [81]. A recent study aims to ensure firmware updates that could be deployed and executed on all IoT devices within given time ranges [81]. This solution is evaluated on three IoT platforms (e.g., HummingBoard Edge, Raspberry Pi Compute Module 3, and Nucleo-L476RG) only. However, IoT devices and platforms have a broad class, several problems are needed to be investigated. Thus, there is a plenty of room for further development to address this issue, which has great practical value for securing the data center operation.

5 CONCLUSION

The prominent features of IoT devices enable its wide deployment in the modern data center industry varying from cloud data centers, to edge data centers, and end users on the edge. This broad integration of IoT devices with data center deployments is a double-edged

sword – it significantly enhances the efficiency of daily operation and enables intelligent management while introducing potential security issues for modern data centers.

This paper is among the first to provide a preliminary survey on the most recent IoT security issues for modern data centers. We first introduce the basics of modern data centers and IoT and explain how IoT affects the data center based on an example of data center deployments. By reviewing the recent publications in the top security conferences, we summarize the recent IoT attacks as well as the newly discovered vulnerabilities, and explain the possible consequences for a data center. Finally, we go over some cybersecurity tools and identify challenges and issues for enhancing the security of a data center from the perspectives of attack detection, vulnerability management, and system recovery.

REFERENCES

[1] ACM. 2022. ACM Conference on Computer and Communications Security (CCS). http://www.sigsac.org/ccs.html Last accessed 23 Feb 2022 .

[2] Luca Allodi and Fabio Massacci. 2014. Comparing Vulnerability Severity and Exploits Using Case-Control Studies. *ACM Transactions on Information and System Security (TISSEC)* 17, 1 (2014), 1–20.

[3] Kenneth Alperin, Allan Wollaber, Dennis Ross, Pierre Trepagnier, and Leslie Leonard. 2019. Risk Prioritization by Leveraging Latent Vulnerability Features in a Contested Environment. In *Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security*. ACM, New York,NY,United States, 49–57.

[4] Omar Alrawi, Charles Lever, Kevin Valakuzhy, Kevin Snow, Fabian Monrose, Manos Antonakakis, et al. 2021. The Circle Of Life: A Large-Scale Study of the IoT Malware Lifecycle. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX, Virtual Event, 3505–3522.

[5] Md Monowar Anjum, Shahrear Iqbal, and Benoit Hamelin. 2021. Analyzing the Usefulness of the DARPA OpTC Dataset in Cyber Threat Detection Research. In *Proceedings of the 26th ACM Symposium on Access Control Models and Technologies*. ACM, Virtual Event, 27–32.

[6] Manos Antonakakis, Tim April, Michael Bailey, Matt Bernhard, Elie Bursztein, Jaime Cochran, Zakir Durumeric, J Alex Halderman, Luca Invernizzi, Michalis Kallitsis, et al. 2017. Understanding the Mirai Botnet. In *26th USENIX security symposium (USENIX Security 17)*. USENIX, Vancouver, BC, Canada, 1093–1110.

[7] Luigi Atzori, Antonio Iera, and Giacomo Morabito. 2010. The Internet of Things: A Survey. *Computer networks* 54, 15 (2010), 2787–2805.

[8] Luiz André Barroso, Urs Hölzle, and Parthasarathy Ranganathan. 2018. The Datacenter As a Computer: Designing Warehouse-scale Machines. *Synthesis Lectures on Computer Architecture* 13, 3 (2018), i–189.

[9] BehrTech Blog. 2020. IoT for Data Center Infrastructure Management: 5 Critical Applications. https://behrtech.com/blog/iot-for-data-center-infrastructure-management-5-critical-applications/ Last accessed 28 Feb 2022 .

[10] Kashif Bilal, Saif Ur Rehman Malik, Osman Khalid, Abdul Hameed, Enrique Alvarez, Vidura Wijaysekara, Rizwana Irfan, Sarjan Shrestha, Debjyoti Dwivedy, Mazhar Ali, et al. 2014. A Taxonomy and Survey on Green Data Center Networks. *Future Generation Computer Systems* 36 (2014), 189–208.

[11] Nadia Chaabouni, Mohamed Mosbah, Akka Zemmari, Cyrille Sauvignac, and Parvez Faruki. 2019. Network Intrusion Detection for IoT Security Based on Learning Techniques. *IEEE Communications Surveys & Tutorials* 21, 3 (2019), 2671–2701.

[12] Jieun Choi, Hae-Yong Yang, and Dong-Ho Cho. 2020. Tempest Comeback: A Realistic Audio Eavesdropping Threat on Mixed-signal SoCs. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. ACM, Virtual Event, 1085–1101.

[13] Chun-Jen Chung, Pankaj Khatkar, Tianyi Xing, Jeongkeun Lee, and Dijiang Huang. 2013. NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems. *IEEE transactions on dependable and secure computing* 10, 4 (2013), 198–211.

[14] CJ Arlotta. 2014. Gartner: Data Centers Must Prepare for the IoT. https://www.channelfutures.com/business-models/gartner-data-centers-must-prepare-for-the-iot Last accessed 23 Feb 2022 .

[15] Microsoft Corp. 2021. Datacenter Threat, Vulnerability, and Risk Assessment. https://docs.microsoft.com/en-us/compliance/assurance/assurance-threat-vulnerability-risk-assessment Last accessed 4 March 2022 .

[16] SpaceDC Corp. 2021. Consequences of An Inadequate Data Center Security. https://spacedc.com/consequences-of-an-inadequate-data-center-security/ Last accessed 5 March 2022 .

[17] Tenable Corp. 2021. Risk-based Vulnerability Management: Understanding Vulnerability Risk With Threat Context and Business Impact. https://www.tenable.com/risk-based-vulnerability-management Last accessed 4 March 2022 .

[18] Vittorio Cozzolino, Nikolai Schwellnus, Jörg Ott, and Aaron Yi Ding. 2020. UIDS: Unikernel-based Intrusion Detection System for the Internet of Things. In *Proceeding of NDSS Workshop Decentralized IoT Systems and Security*. NDSS, San Diego, California, USA, 1–6.

[19] Cyble Inc. 2022. Data Center Infrastructure Management Tools Facing The Risk Of Cyberattacks. https://blog.cyble.com/2022/01/27/data-centers-facing-risk-of-cyberattacks/ Last accessed 28 Feb 2022 .

[20] Li Da Xu, Wu He, and Shancang Li. 2014. Internet of Things in Industries: A Survey. *IEEE Transactions on industrial informatics* 10, 4 (2014), 2233–2243.

[21] Dan Swinhoe. 2021. Iranian APT campaign hosted in Dutch data centers. https://www.datacenterdynamics.com/en/news/iranian-apt-campaign-hosted-dutch-data-centers/ Last accessed 1 March 2022 .

[22] Miyuru Dayarathna, Yonggang Wen, and Rui Fan. 2015. Data Center Energy Consumption Modeling: A Survey. *IEEE Communications Surveys & Tutorials* 18, 1 (2015), 732–794.

[23] Kelley Dempsey, Eduardo Takamura, Paul Eavy, and George Moore. 2020. *Automation Support for Security Control Assessments: Software Vulnerability Management*. Technical Report. National Institute of Standards and Technology.

[24] Keval Doshi, Mahsa Mozaffari, and Yasin Yilmaz. 2019. Rapid: Real-time Anomaly-based Preventive Intrusion Detection. In *Proceedings of the ACM Workshop on Wireless Security and Machine Learning*. ACM, Miami, FL, USA, 49–54.

[25] Xiaotao Feng, Ruoxi Sun, Xiaogang Zhu, Minhui Xue, Sheng Wen, Dongxi Liu, Surya Nepal, and Yang Xiang. 2021. Snipuzz: Black-box Fuzzing of IoT Firmware Via Message Snippet Inference. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. ACM, Virtual Event, 337–350.

[26] Leylane Ferreira, Patricia Takako Endo, Daniel Rosendo, Guto Leoni Santos, Demis Gomes, André Luis Cavalcanti Moreira, Glauco Estácio Goncalves, Judith Kelner, Djamel Sadok, Amardeep Mehta, et al. 2020. Standardization Efforts for Traditional Data Center Infrastructure Management: the Big Picture. *IEEE Engineering Management Review* 48, 1 (2020), 92–103.

[27] Dinei Florêncio, Cormac Herley, and Baris Coskun. 2007. Do Strong Web Passwords Accomplish Anything? *HotSec* 7, 6 (2007), 159.

[28] Chenglong Fu, Qiang Zeng, and Xiaojiang Du. 2021. HAWatcher: Semantics-Aware Anomaly Detection for Appified Smart Homes. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX, Virtual Event, 4223–4240.

[29] Jiechao Gao, Haoyu Wang, and Haiying Shen. 2020. Task Failure Prediction in Cloud Data Centers Using Deep Learning. *IEEE transactions on services computing* (2020).

[30] Gartner. 2021. Top Priorities for IT: Leadership Vision for 2021. https://www.gartner.com/en/publications/security-risk-top-priorities-for-it-leadership-vision-2021 Last accessed 4 March 2022 .

[31] Gartner Corp. 2014. Gartner Says the Internet of Things Will Transform the Data Center. https://www.gartner.com/en/information-technology/insights/internet-of-things Last accessed 23 Feb 2022 .

[32] Gartner Corp. 2021. Gartner Predicts the Future of Cloud and Edge Infrastructure. https://www.gartner.com/smarterwithgartner/gartner-predicts-the-future-of-cloud-and-edge-infrastructure Last accessed 23 Feb 2022 .

[33] Sukhpal Singh Gill, Shreshth Tuli, Minxian Xu, Inderpreet Singh, Karan Vijay Singh, Dominic Lindsay, Shikhar Tuli, Daria Smirnova, Manmeet Singh, Udit Jain, et al. 2019. Transformative effects of IoT, Blockchain and Artificial Intelligence on Cloud Computing: Evolution, Vision, Trends and Open Challenges. *Internet of Things* 8 (2019), 100118.

[34] Xueyuan Han, Thomas Pasquier, Adam Bates, James Mickens, and Margo Seltzer. 2020. Unicorn: Runtime Provenance-based Detector for Advanced Persistent Threats. In *Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2020*. NDSS, San Diego, CA, USA, 1–18.

[35] Stephen Herwig, Katura Harvey, George Hughey, Richard Roberts, and Dave Levin. 2019. Measurement and Analysis of Hajime, A Peer-to-peer IoT Botnet. In *Network and Distributed Systems Security (NDSS) Symposium*. NDSS, San Diego, California, United State.

[36] Kate Highnam, Kevin Angstadt, Kevin Leach, Westley Weimer, Aaron Paulos, and Patrick Hurley. 2016. An Uncrewed Aerial Vehicle Attack Scenario and Trustworthy Repair Architecture. In *2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop (DSN-W)*. IEEE, Toulouse, France, 222–225.

[37] Martin Husák, Jana Komárková, Elias Bou-Harb, and Pavel Čeleda. 2018. Survey of Attack Projection, Prediction, and Forecasting in Cyber Security. *IEEE Communications Surveys & Tutorials* 21, 1 (2018), 640–660.

[38] IEEE. 2022. IEEE Symposium on Security and Privacy. http://www.ieee-security.org/TC/SP-Index.html Last accessed 23 Feb 2022 .

[39] Kyle Ingols, Richard Lippmann, and Keith Piwowarski. 2006. Practical Attack Graph Generation for Network Defense. In *22nd Annual Computer Security Applications Conference (ACSAC'06)*. IEEE, Miami Beach, FL, USA, 121–130.

[40] Intel Corp. 2013. IPMI Specification, V2.0, Rev. 1.1: Document. https://www.intel.com/content/www/us/en/products/docs/servers/ipmi/ipmi-second-gen-interface-spec-v2-rev1-1.html Last accessed 4 March 2022 .

[41] International Organization for Standardization. 2018. ISO/IEC 27000:2018 Information Technology, Security Techniques, Information Security Management Systems, Overview and Vocabulary. https://www.iso.org/standard/73906.html Last accessed 4 March 2022 .

[42] Xibo Jin, Fa Zhang, Athanasios V Vasilakos, and Zhiyong Liu. 2016. Green Data Centers: A Survey, Perspectives, and Future Directions. *arXiv preprint arXiv:1608.00687* (2016).

[43] Minho Jo, Longzhe Han, Nguyen Duy Tan, and Hoh Peter In. 2015. A Survey: Energy Exhausting Attacks in MAC Protocols in WBANs. *Telecommunication Systems* 58, 2 (2015), 153–164.

[44] Kyo Kim, Siddhartha Nalluri, Ashish Kashinath, Yu Wang, Sibin Mohan, Miroslav Pajic, and Bo Li. 2020. Security Analysis Against Spoofing Attacks for Distributed UAVs. In *Proceeding of the Network and Distributed System Security Symposium (NDSS)*. NDSS, San Diego, California, USA.

[45] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. 2017. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE internet of things journal* 4, 5 (2017), 1125–1142.

[46] Liang Liu, Hao Wang, Xue Liu, Xing Jin, Wen Bo He, Qing Bo Wang, and Ying Chen. 2009. GreenCloud: A New Architecture for Green Data Center. In *Proceedings of the 6th International Conference Industry Session on Autonomic Computing and Communications Industry Session*. ACM, Barcelona,Spain, 29–38.

[47] Qiang Liu, Yujun Ma, Musaed Alhussein, Yin Zhang, and Limei Peng. 2016. Green Data Center with IoT Sensing and Cloud-assisted Smart Temperature Control System. *Computer Networks* 101 (2016), 104–112.

[48] Gordon Fyodor Lyon. 2008. *Nmap Network Scanning: The official Nmap Project Guide to Network Discovery and Security Scanning*. Insecure. Com LLC (US), United States.

[49] Sadegh M Milajerdi, Rigel Gjomemo, Birhanu Eshete, R Sekar, and VN Venkatakrishnan. 2019. Holmes: Real-time Apt Detection Through Correlation of Suspicious Information Flows. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 1137–1152.

[50] MITRE. 2021. CVE Program. https://cve.mitre.org/ Last accessed 3 March 2022 .

[51] Mitre Organization. 2022. Bluetooth Vulnerabilities. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=bluetooth Last accessed 3 March 2022 .

[52] Mitre Organization. 2022. Data Center Vulnerabilities. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=%22data+center%22 Last accessed 3 March 2022 .

[53] Susan Moore. 2021. Security and Risk Leaders Should Tie Vulnerability Management Practices to Their Organization's Specific Needs, Not a Mythical Standard. https://www.gartner.com/smarterwithgartner/how-to-set-practical-timeframes-to-remedy-security-vulnerabilities/ Last accessed 4 March 2022 .

[54] Muhammad Nouman Nafees, Neetesh Saxena, Pete Burnap, and Bong Jun Choi. 2020. Impact of Energy Consumption Attacks on LoRaWAN-enabled Devices in Industrial Context. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. ACM, London, UK, 2117–2119.

[55] NDSS. 2022. Network and Distributed System Security (NDSS) Symposium. https://www.ndss-symposium.org/ Last accessed 23 Feb 2022 .

[56] Rajvardhan Oak, Min Du, David Yan, Harshvardhan Takawale, and Idan Amit. 2019. Malware Detection on Highly Imbalanced Data Through Sequence Modeling. In *Proceedings of the 12th ACM Workshop on artificial intelligence and security*. ACM, London, United Kingdom, 37–48.

[57] National Institute of Standards and Technology. 2021. Advanced Persistent Threat(APT). https://csrc.nist.gov/glossary/term/advanced_persistent_threat Last accessed 4 March 2022 .

[58] Xinming Ou, Sudhakar Govindavajhala, Andrew W Appel, et al. 2005. MulVAL: A Logic-based Network Security Analyzer.. In *USENIX security symposium*, Vol. 8. USENIX, Baltimore, MD, USA, 113–128.

[59] Gopika Premsankar, Mario Di Francesco, and Tarik Taleb. 2018. Edge Computing for the Internet of Things: A Case Study. *IEEE Internet of Things Journal* 5, 2 (2018), 1275–1284.

[60] Deepak Puthal, Surya Nepal, Rajiv Ranjan, and Jinjun Chen. 2016. Threats to Networking Cloud and Edge Datacenters in the Internet of Things. *IEEE Cloud Computing* 3, 3 (2016), 64–71.

[61] PYMNTS. 2021. Kaspersky Detects 1.5B IoT Cyberattacks This Year. https://www.pymnts.com/news/security-and-risk/2021/kaspersky-detects-iot-cyberattacks-double-last-year/ Last accessed 28 Feb 2022 .

[62] Tie Qiu, Jiancheng Chi, Xiaobo Zhou, Zhaolong Ning, Mohammed Atiquzzaman, and Dapeng Oliver Wu. 2020. Edge Computing in Industrial Internet of Things: Architecture, Advances and Challenges. *IEEE Communications Surveys & Tutorials* 22, 4 (2020), 2462–2488.

[63] Rapid 7 Corp. 2022. What is A Spoofing Attack? https://www.rapid7.com/fundamentals/spoofing-attacks/ Last accessed 3 March 2022 .

[64] Carl Sabottke, Octavian Suciu, and Tudor Dumitraș. 2015. Vulnerability Disclosure in the Age of Social Media: Exploiting Twitter for Predicting Real-World Exploits. In *24th USENIX Security Symposium (USENIX Security 15)*. USENIX, Washington, D.C., USA, 1041–1056.

[65] Sagar Samtani, Hongyi Zhu, and Hsinchun Chen. 2020. Proactively Identifying Emerging Hacker Threats from the Dark Web: A Diachronic Graph Embedding Framework (D-GEF). *ACM Transactions on Privacy and Security (TOPS)* 23, 4 (2020), 1–33.

[66] David Davis Scott D. Lowe, James Green. 2016. *Building a Modern Data Center Principles and Strategies of Design* (1st. ed.). Atlantis Computing, Bluffton, SC.

[67] Shelby Hiter. 2021. What is an Advanced Persistent Threat (APT) Attack? https://www.cioinsight.com/security/apt-attack/ Last accessed 1 March 2022 .

[68] Saleh Soltan, Prateek Mittal, and H Vincent Poor. 2018. BlackIoT:IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX, Baltimore, MD, USA, 15–32.

[69] Gaurav Somani, Manoj Singh Gaur, Dheeraj Sanghi, and Mauro Conti. 2016. DDoS Attacks in Cloud Computing: Collateral Damage to Non-targets. *Computer Networks* 109 (2016), 157–171.

[70] Maria Stoyanova, Yannis Nikoloudakis, Spyridon Panagiotakis, Evangelos Pallis, and Evangelos K Markakis. 2020. A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues. *IEEE Communications Surveys & Tutorials* 22, 2 (2020), 1191–1221.

[71] Vijey Thayananthan and Aiiad Albeshri. 2015. Big Data Security Issues Based on Quantum Cryptography and Privacy with Authentication for Mobile Data Center. *Procedia Computer Science* 50 (2015), 149–156.

[72] The Forum of Incident Response and Security Teams (FIRST). 2021. Common Vulnerability Scoring System SIG. https://www.first.org/cvss/ Last accessed 3 March 2022 .

[73] The National Institute of Standards and Technology. 2020. NVD: National Vulnerability Database. https://nvd.nist.gov/general Last accessed 25 August 2020.

[74] Liang Tong, Yong Li, and Wei Gao. 2016. A Hierarchical Edge Cloud Architecture for Mobile Computing. In *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications*. IEEE, San Francisco, CA, USA, 1–9.

[75] USENIX. 2022. USENIX Security Symposia. https://www.usenix.org/conferences/byname/108 Last accessed 23 Feb 2022.

[76] Haohuang Wen, Zhiqiang Lin, and Yinqian Zhang. 2020. Firmxray: Detecting Bluetooth Link Layer Vulnerabilities From Bare-metal Firmware. In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*. ACM, Virtual Event, 167–180.

[77] Wiki. 2021. Nessus. https://en.wikipedia.org/wiki/Nessus_(software) Last accessed 8 June 2021.

[78] Wiki. 2022. Denial-of-service Attack. https://en.wikipedia.org/wiki/Denial-of-service_attack Last accessed 1 March 2022.

[79] YM Wu, P Cao, Alexander Withers, Zbigniew T Kalbarczyk, and Ravishankar K Iyer. 2020. Mining Threat Intelligence From Billion-scale SSH Brute-force Attacks. In *Proceeding of the Network and Distributed System Security Symposium (NDSS)*. NDSS, San Diego, California, USA.

[80] Xahive Corp. 2016. Side Channel - TEMPEST Attacks. https://2016.export.gov/canada/build/groups/public/@eg_ca/documents/webcontent/eg_ca_106274.pdf Last accessed 28 Feb 2022.

[81] Meng Xu, Manuel Huber, Zhichuang Sun, Paul England, Marcus Peinado, Sangho Lee, Andrey Marochko, Dennis Mattoon, Rob Spiger, and Stefan Thom. 2019. Dominance As A New Trusted Computing Primitive for the Internet of Things. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, United State, 1415–1430.

[82] Chi Yang, Deepak Puthal, Saraju P Mohanty, and Elias Kougianos. 2017. Big-sensing-data Curation for the Cloud is Coming: A Promise of Scalable Cloud-data-center Mitigation for Next-generation IoT and Wireless Sensor Networks. *IEEE Consumer Electronics Magazine* 6, 4 (2017), 48–56.

[83] Wei Yu, Fan Liang, Xiaofei He, William Grant Hatcher, Chao Lu, Jie Lin, and Xinyu Yang. 2017. A Survey on the Edge Computing for the Internet of Things. *IEEE access* 6 (2017), 6900–6919.

[84] Bin Yuan, Yan Jia, Luyi Xing, Dongfang Zhao, XiaoFeng Wang, and Yuqing Zhang. 2020. Shattered Chain of Trust: Understanding Security Risks in Cross-Cloud IoT Access Delegation. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX, Virtual Event, 1183–1200.

[85] Zhen Zeng, Zhun Yang, Dijiang Huang, and Chun-Jen Chung. 2021. LICALITY–Likelihood and Criticality: Vulnerability Risk Prioritization Through Logical Reasoning and Deep Learning. *IEEE Transactions on Network and Service Management* (2021).

[86] Jiao Zhang, F Richard Yu, Shuo Wang, Tao Huang, Zengyi Liu, and Yunjie Liu. 2018. Load Balancing in Data Center Networks: A Survey. *IEEE Communications Surveys & Tutorials* 20, 3 (2018), 2324–2352.

[87] Wei Zhou, Yan Jia, Yao Yao, Lipeng Zhu, Le Guan, Yuhang Mao, Peng Liu, and Yuqing Zhang. 2019. Discovering and Understanding the Security Hazards in the Interactions between {IoT} Devices, Mobile Apps, and Clouds on Smart Home Platforms. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX, Santa Clara, CA, USA, 1133–1150.

[88] Chaoshun Zuo, Haohuang Wen, Zhiqiang Lin, and Yinqian Zhang. 2019. Automatic Fingerprinting of Vulnerable BLE IoT Devices with Static UUIDs from Mobile Apps. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. ACM, London, UK, 1469–1483.