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

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
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.).

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...
As IoT device design developed, the IoT integrated design brings new security issues related to the TEMPEST 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 typical power circuit of the 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].

**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 TEMPEST 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].

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

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

**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
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]. 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
We first introduce the basics of modern data centers and IoT and vulnerability management, and system recovery.

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


