Applied Laser Technology

Vol. 29, No.2,April (2022), pp.01–05

Analyzing how thieves focus on certain components of IoT networks

Dr D Arun Kumar[1,] A Valli Basha [2] S L Pratap Reddy[3], R V Sree Hari[4]
[2] Asst. Professor, Department of ECE, K. S. R. M College of Engineering(A), Kadapa
[1,3,4] Associate Professor, Department of ECE, K. S. R. M College of Engineering(A), Kadapa

Abstract

Information security, decentralized decision-making systems, and analysis of the Internet of Things (IoT), as well as the possibility of edge computing to minimize traffic transmission, are all topics covered in this article. There was extensive investigation into the vectors of attack on IoT systems, and therefore, protective measures were proposed.

keywords

Internet of Things; Cybersecurity; Intrusion; Defense; Edge Computing.

Introduction

The development and use of Internet of Things (IoT) technologies have expanded greatly in recent years. Researchers in the Internet of Things industry have discovered that the number of linked devices is increasing at a rapid rate. The number of connected devices is expected to grow from the current 21 billion to more than 50 billion in only a few years [1, 2]. Because of the proliferation of IoT devices and the lack of security they provide, information technology security experts are concerned [3, 4, 5, 6, 7]. They claim that fraudsters are given a better chance of success due to the rise of Internet-connected devices that lack adequate security measures. There have been several reported cases of failed Internet of Things systems. This is a crucial responsibility since these tools are used at essential facilities.

As new tools and methods become more widely available, new cyberthreats emerge. Businesses are always trying to perfect the protection systems they've developed and find new ways to implement them. The development of information technology necessitates alterations in the field of information security. As a result of technological progress, different cybersecurity concerns may be addressed. Edge computing has made significant strides, with the ability to remotely monitor and analyse data from IoT devices being one of the most notable advancements. The primary advantage of this approach is that it removes the need to transfer data to a centralized location or the cloud for processing and speedy decision making. The Internet of Things (IoT) and edge computing might operate well together in a variety of contexts [8]. This includes hospitals, temperature control systems, "smart" buildings, municipal or regional infrastructure management, commerce and logistics networks, and more. There is a lot of promise for edge computing to be used in network security monitoring and access control systems. This method is excellent for preventing the spread of malware and other forms of cyberattacks. When you get a signal from one of your numerous IoT devices, you can immediately assess the situation and decide whether or not to issue an alarm, move the "object" to quarantine, or isolate it altogether. As the number of Internet of Things (IoT) devices continues to grow, it will become more difficult to get the vast amounts of data they produce to centralized data centers or the cloud for analysis and storage, making edge computing increasingly important in many areas of the digital society. The study of edge computing for traffic reduction, data storage, resources, and security in the Internet of Things is now essential for the development of digital society and humanity's entry into the fourth industrial revolution (Industry 4.0) [9].

Theoretical Contextualization

Examining the aforementioned works [1, 2, 10] confirms the benefits of these devices and technologies and the progression of mankind towards adopting Industry 4.0, highlighting the significance of IoT study. In [1, 2, 3], the authors highlight the rapid pace at which the Internet of Things is being embraced by many sectors of today's information society. Ammerman [1] testified that management choices were aided by using cloud computing to interpret, analyze, and store sensor data. As the number of Internet-connected devices continues to explode, putting a pressure on both network bandwidth and cloud storage capacity (in the billions of gigabytes), edge computing is no longer a nice-to-have. The author discusses when and why edge computing and cloud technologies are both useful—and even necessary—in the corporate world. Edge computing is the most

important aspect of the Internet of Things if you want to reduce latency and increase the reliability of your deployed systems [1]. Information security models for the Internet of Things are outlined, the need for IoT security is established, and lessons learned from research on the centralization and decentralization of such systems are presented. The need to protect data in its totality is urgent. Network security, authentication, encryption, attack security, security analytics, threat forecasting, interface protection, and delivery methods are only a few of the eight fundamental security technologies outlined by Byler [3]. In [4, 5, 6, 10, 11, 12], the potential benefits and threats of the Internet of Things (IoT) are examined. These works demonstrate the significance of security considerations, safe areas, and fundamental conceptual approaches to security. Numerous disruptive cyberattacks have occurred, and the frequency with which hackers strike is rising [7, 13, 14, 15]. Losses from incidents that might total billions of dollars underline the gravity of the situation.

Figure 1: IoT security environment

When looking at both mobile and cloud features, HP's experts have discovered an average of 25 unique security issues per device [13]. HP's experts have concluded that a secure IoT solution is not now available. Because of the overall increase in targeted attacks, the particular threat to the IoT is often overlooked. Our IoT friends turn traitor and provide hackers complete access to our lives once they take an interest in us. Hardware, software, and network/communications device developers are racing to discover a fix for the widespread issue [15]. The Internet of Things (IoT) security framework was developed by Cisco Systems, a forerunner in the IoT security domain and a significant contributor to the IoT model's progress at the World IoT Forum [13]. Figure 1 depicts the security infrastructure supporting the IoT's logical architecture. Cisco's IoT paradigm is more basic than the one proposed by the World IoT Forum. Figure 1 illustrates how specialized functional areas of security sit atop the four levels of the IoT paradigm. Also, the Cisco paper proposes an IoT security concept that explains how authentication, authorisation, network policy, and security analytics all go together to form the IoT security feature. The human race's adoption of Industry 4.0 presents new challenges and opportunities for Ukraine [10]. In the era of Industry 4.0, attacks on government infrastructure might have disastrous results. This effort assumes more relevance in the design of temporary protection of the perimeter of the regime object when supplies are limited, severe weather is anticipated, and the terrain is unknown. The proliferation of wireless communication techniques inside the system creates perfect settings for a successful cyberattack, and the majority of cyberattacks come from mobile devices. Numerous studies [4, 5, 6, 10, 11, 12] have identified entry points (access) into the corporate network as the primary vector via which hackers obtain unauthorized access to the network or use the network to launch a DDoS assault. Due to the vast number of sensors connected to the system, wireless networks, cloud services, etc. cannot provide a reliable perimeter of cybersecurity of the item. Another issue (for businesses) is the leakage of private customer data. Due to the seriousness of the situation, machine learning and AI technologies that are employed to address cyber threats play a dual function (the algorithms utilized may both counteract and produce cyber-attacks). There will always be new forms of cyber threat, and the only way to counter them is through state-of-the-art computer systems.

Results

We've broken down the hardware of our wireless Internet of Things (IoT) research system into the following categories [3, 4, 11, 6]:

1. communication subsystem (wireless communication in the sensor network, includes a radio receiver),

2. computing subsystem (data processing, node functionality),

3. sensor subsystem (network connection with the “outside world”),

4. power subsystem. Tasks facing the system to the hardware:

• low electricity consumption,

• the ability to work with a large number of nodes at relatively short distances,

• relatively low cost,

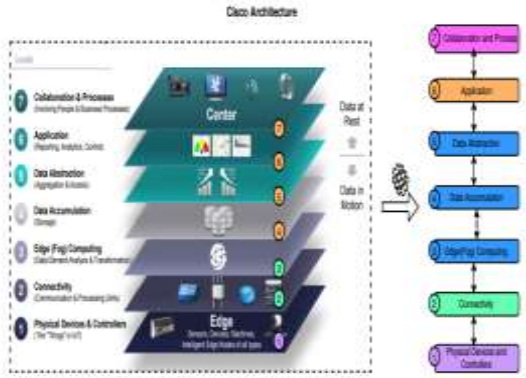

Figure 2: Cisco IoT Architecture

• work autonomously and without maintenance,

• have a camouflage effect,

• be resistant to the environment.

We opted for Cisco's 7-tier model for IoT systems' structure (figure 2). The adoption of IoT systems to guard the periphery of the regime object raises the problem of cybersecurity in light of the fact that sensor networks are susceptible to several assaults. During the movement of cargo/persons/reconnaissance operation, it is assumed that temporary perimeter protection must be carried out. Figure 3 displays a simulation of a single IoT perimeter security zone created in Cisco Packet Tracer. A temporary perimeter security system zone may be set up with the help of the gadgets included in this plan. Also modelled a typical fire alarm system for a single room using the garage as an example (figure 4). The equipment is quite standard. In order to investigate possible cyber dangers and offer suggestions for the safety of IoT components, we have developed computer models, as shown in figures 3 and 4. Future research will reveal the outcomes of modelling and preventing cyberattacks. Through careful system modelling, we were able to identify the following as the most pressing cybersecurity concerns:

• communication security,

• protection of the devices themselves,

• control over the operation of devices,

• control of network interaction

Vol. 29, No.2,April (2022), pp.01–05

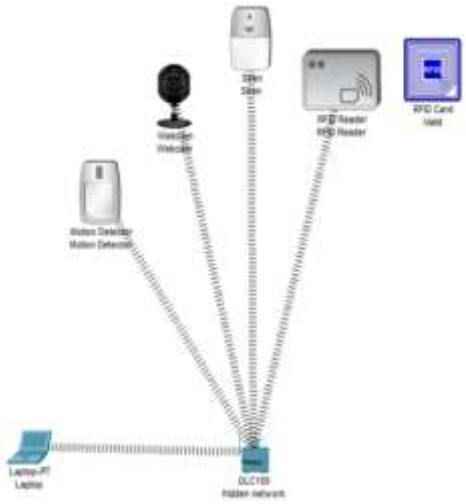

Figure 3: Cluster protection zone

As a result of research and analysis of the most likely attacks on simulated systems, the following classification of attacks is proposed (figure 5):

- Denial-of-Service (DoS) (*D*):
  - physical level (*H*):
    - obstacle attack (H_1)
    - attack of interference in the IoT system (H_2)
  - channel level (*C*):
    - collision attack (C_1)
- attacks on routing protocols (*R*):
  - "Black Hole" attack (R_1)
  - selective forwarding attack (R_2)
  - "Rapid onslaught" attack (R_3)
  - "Funnel" attack (R_4)

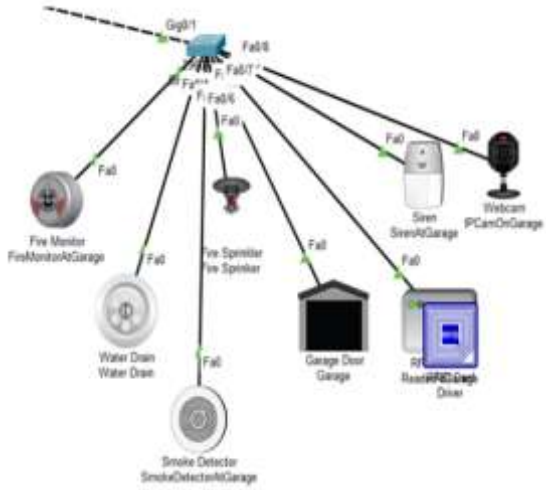

Figure 4: Scheme of fire alarm system of a separate room on the example of a garage

- Sybil attack (R_5)
- "wormholes" attack (R_6)
- flood attack (R_7)

- attacks at the transport level (T):
  - avalanche attack (T_1)
  - desynchronization attack (T_2)
- attacks on data aggregation (G);
- privacy attacks (P).

Attacks can be represented in the form of open classification groups. $D = H \cup C$ – a set of attacks that lead to denials of service, involves combining sets of attacks at the physical and channel level. Many attacks that lead to denials of service at the physical level:

$$H = \bigcup_{i=1}^{n} H_i$$

Figure 5: Attacks on IoT system components

The set of attacks that lead to denial-of-service link-level:

$$C = \bigcup_{k=1}^{z} C_k$$

The set of attacks on routing protocols:

$$R = \bigcup_{v=1}^{s} R_v$$

The open classification grouping of transport layer attacks is presented in the form of a set:

$$G = \bigcup_{j=1}^{m} G_j$$

The set of attacks on privacy:

$$P = \bigcup_{\gamma=1}^{\delta} P_\gamma$$

In general, attacks can be represented as a union of all classification groups:

$$A = D \bigcup R \bigcup T \bigcup G \bigcup P$$

Let's analyse each attack that is part of the classification group.

A physical DoS assault. When an adversary attempts to disable a network or wipe out a network security service, they are launching a Denial-of-Service assault. DoS attacks in IoT systems may happen anywhere throughout the protocol stack, can impact many layers at once, and can take advantage of the interplay between them. The radio frequencies on which the system relies may be disrupted to launch a physical DoS assault. A single attacker node might cause a complete or partial network outage in this scenario (for example, blocking data transmission). Our approach relies heavily on the IoT's ability to identify an attack based on the presence of a sensor (in this example, a sensor/camera around a security item) and an effort to physically access it. An attacker may then either exploit the device to break into the network or destroy it, attempt to replace the data, get access to private information (including cryptographic keys), or all of the above.

DDoS attacks often target whole channels. The goal of a channel-level denial-of-service collision attack is often to exhaust the resources of nodes. As a result of this attack, various MAC protocols experience exponential latency and packet retransmission processes. Because of this, when a packet sustains extensive damage, the node will waste energy trying to employ error correction codes to recover the broken bits. A "collision" at the frame's conclusion is another kind of attack that causes the whole packet to be resent. Sending a Request for Transmission Suppression (RTS) message to a base station or neighbouring node can be a form of attack supported by the IEEE 802.11 protocols. This causes the receiving node to stop transmitting data to the sending nodes for the amount of time specified by the RTS message while it processes the RTS and sends a CTS message. Methods including a handshake may also be used.

Conclusions

From this study, we were able to generalise cyber risks to the individual parts of IoT systems. The results show that network nodes are the primary target of cyber assaults, and that the usage of wireless technologies for inter-system communication fosters an environment conducive to such attacks. Based on the newest technology means, qualified staff, control processes, administrative rules, and their strict adherence, it has been decided that today's multi-stage complicated protection systems are being implemented. By analysing attacks, we were able to compile a list of them and investigate their implementation details. Based on the findings of the analysis and generalisation, suggestions have been made to defend the individual nodes that make up the Internet of Things.

References

[1] G. Immerman, The importance of edge computing for the iot, 2020. URL: https://www. machinemetrics.com/blog/edge-computing-iot.

[2] S. Khomich, A. Fedosiuk, M. Kulikovsky, Research of system of iot devices information security, Digital technologies 18 (2015) 166–171.

[3] J. Blyler, 8 critical iot security technologies, 2020. URL: https://www.electronicdesign. com/industrial-automation/article/21805420/8-critical-iot-security-technologies.

[4] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, D. Qiu, Security of the internet of things: perspectives and challenges, Wireless Networks 20 (2014) 2481–2501. doi:10.1007/ s11276-014-0761-7.

[5] D. Kuznetsov, L. Ryabchina, Information security of the internet of things systems, Bulletin of Kryvyi Rih National University 49 (2019) 80–83.

[6] O. Turanska, Development of methods of information protection in wireless sensor networks: master's thesis, Master's thesis, NTU of Ukraine "KPI named after Igor Sikorsky", 2018.

[7] C. Systems, The internet of things reference model, 2014. URL: http://cdn.iotwf.com/ resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf.

[8] A. Herts, I. Tsidylo, N. Herts, L. Barna, S.-I. Mazur, Photosynq - cloud platform powered by iot devices, E3S Web of Conferences 166 (2020). doi:10.1051/e3sconf/202016605001.

[9] S. Shokaliuk, Y. Bohunenko, I. Lovianova, M. Shyshkina, Technologies of distance learning for programming basics on the principles of integrated development of key competences, CEUR Workshop Proceedings 2643 (2020) 548–562.

[10] S. Gnatyuk, Cybersecurity in the context of the fourth industrial revolution (industry 4.0): challenges and opportunities for ukraine, 2019. URL: https://niss.gov.ua/doslidzhennya/ informaciyni-strategii/kiberbezpeka-v-umovakh-rozgortannya-chetvertoi-promislovoi.

[11] A. Vovk, Methods of information security IoT, Master's thesis, NTU of Ukraine "KPI named after Igor Sikorsky", 2018.

[12] O. Korchenko, M. Alexander, R. Odarchenko, A. Nadzhi, O. Petrenko, Analysis of threats.and mechanisms for information security in sensor networks, Information protection 1 (2016) 48–56.

[13] H. Packard, Hp study reveals 70 percent of internet of things devices vulnerable to attack, 2020. URL: https://www8.hp.com/us/en/hp-news/press-release.html?id=1744676.

[14] J. Frahim, C. Pignataro, J. Apcar, M. Morrow, Securing the Internet of Things: A Proposed Framework, 2015. URL: http://web.archive.org/web/20210323170935/https://tools. cisco.com/security/center/resources/secure_iot_proposed_framework.

[15] M. G. dos Santos, D. Ameyed, F. Petrillo, F. Jaafar, M. Cheriet, Internet of things architectures: A comparative study, 2020. URL: https://arxiv.org/pdf/2004.12936.pdf.