Analysis of cyber attacks against Internet of Things infrastructure components

Dr. K. Amit Bindaj
HOD, ECE
SBIT, KHAMMAM
Email: karpurapu.gavasj@gmail.com

Mr. T. Gangadhar
Asst Professor, ECE
SBIT, KHAMMAM
Email: Gangadhar4vlsi@gmail.com

Mr Ch. Gopala Rao
Asst Professor, ECE
SBIT, KHAMMAM
Email: chintala.gopal4@gmail.com

Abstract

This article discusses the Internet of Things (IoT), including its analysis, techniques and means of protection, the potential of employing edge computing to reduce traffic transmission, the decentralisation of decision-making systems, and information security. There was intensive research into the ways in which IoT systems are attacked, and safeguarding suggestions were developed as a result.

keywords

Cybersecurity, intrusion, and defence in an IoT environment; edge computing; IoT. keywords.

Introduction

Internet of Things (IoT) technologies have seen significant growth and deployment in recent years. Researchers in the market for the Internet of Things have found that the total number of connected gadgets is growing at an impressive clip. Even if the present estimate of 21 billion active IoT devices is accurate, that number will rise to over 50 billion in only a few years [1, 2]. IT security professionals are worried about the lack of protection afforded by IoT devices as a result of their growth and broad use [3, 4, 5, 6, 7]. They argue that fraudsters now have more chances thanks to the proliferation of unprotected Internet-connected gadgets. Several instances of IoT systems failing have been documented. In the context of utilising these instruments at vital infrastructure, this is a very important duty.

New cyberthreats are emerging as a result of the proliferation of new technology and techniques. Companies are continually working to standardise, correlate, and apply the protection mechanisms they have created. Adjustments in the area of information security are made as a result of the evolution of information technology. Therefore, various cybersecurity issues may be resolved thanks to the development and advancement of computer technology. One of the most prominent developments in edge computing is the movement towards doing remote monitoring and data processing directly on IoT devices. The key benefit of this method is that it eliminates the need to move all data to a central location or the cloud where it can be processed and decisions can be made quickly. Industry, hospitals, temperature control systems, and "smart" buildings, municipal or regional infrastructure management, commerce and logistics networks, and more may all benefit from the integration of IoT and edge computing [8]. Edge computing's potential in the realm of network security monitoring and access control systems is very exciting. This technique is very useful in stopping the propagation of malware and stopping certain sorts of attacks. The ability to do calculations quickly after receiving a signal means that you may determine whether or not to trigger an alert, relocate the "object" to quarantine, or isolate many IoT devices as needed to avoid network compromise or system failure. Edge computing is essential in many facets of the digital society due to the proliferation of IoT devices, which generates massive volumes of data that are more challenging to send to a data centre or cloud for processing and storage. For the advancement of digital society and humanity's entrance into the fourth industrial revolution (Industry 4.0), the investigation of traffic reduction technologies, data storage, resources, and security in IoT employing edge computing is now a critical endeavour [9].

Contextualization in Theory

The advantages of these devices and technologies, as well as humanity's evolution towards using Industry 4.0, are confirmed by an examination of the aforementioned works [1, 2, 10], demonstrating the importance of IoT research. The authors of [1, 2, 3] discuss the lightning-fast rate at which the Internet of Things is being adopted by diverse

sectors of the modern information society. According to testimony provided by Ammerman [1], cloud computing was first used to process, analyse, and store sensor data before being used to inform management decisions. Edge computing is no longer a luxury but a necessity due to the exponential growth of connected devices and the resulting strain on network bandwidth and cloud storage capacity (measured in the billions of gigabytes). The author explains how edge computing and cloud technologies may work together and how they may even be required in certain situations, particularly in business. If you want to decrease latency and boost the dependability of your deployed systems, then edge computing is the most crucial part of the Internet of Things [1]. Models of the IoT architecture are described, the requirement for IoT security is identified, and findings from studies on the design of information security systems for IoT devices are provided, both centralised and decentralised options being considered. Securing information in its entirety is a pressing concern. With this in mind, Byler [3] outlines eight essential security technologies for protecting the Internet of Things, including: network security, authentication, encryption, attack security, security analytics, threat forecasting, interface protection, and delivery methods. The future of the Internet of Things (IoT) and the dangers it faces are discussed in [4, 5, 6, 10, 11, 12]. Based on their study, these studies corroborate the importance of security concerns, protective zones, and primary conceptual approaches to security. There have been several instances of disruptive cyberattacks, and the frequency with which hackers strike is increasing [7, 13, 14, 15]. Incidents, the losses from which may be estimated in billions of dollars, highlight the seriousness of the issue.

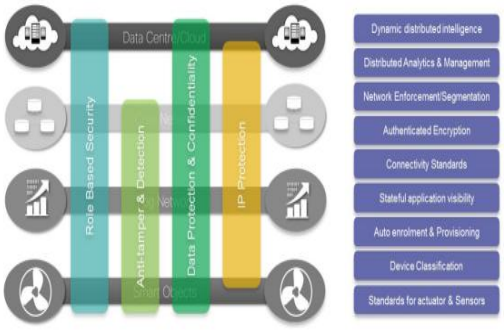

Figure 1: IoT security environment

Experts from HP have found an average of 25 separate security flaws across all of the mobile and cloud components of the devices under study [13]. Unfortunately, HP's specialists have come to the conclusion that a safe IoT system just does not exist at now. The specific risk to the IoT is obscured by the general rise of targeted assaults. Once intruders take an interest in somebody, our IoT companions betray us and provide full access to their owners' worlds. The problem is so serious that manufacturers of hardware, software, and network and communication devices are scrambling to find solutions [15]. Cisco Systems, a pioneer in the IoT security space and a key contributor to the IoT model's evolution at the World IoT Forum, created the IoT security framework, which is now an integral part of the reference model [13]. As can be seen in Figure 1, the IoT's logical structure is accompanied by a security environment. When compared to the World IoT Forum concept, Cisco's IoT model is a simplification. In Figure 1, we can see how the four tiers of the IoT paradigm are topped with specialised functional areas of security. In addition, the Cisco document suggests an IoT security concept that describes the components of the IoT security feature, including authentication, authorisation, network policy, and security analytics. Ukraine has new difficulties and possibilities as a result of humanity's admission into Industry 4.0 [10]. Attacks on government infrastructure in the age of Industry 4.0 might have grave implications. When resources are few, bad weather is expected, and the landscape is unknown, this work takes on added significance in the planning of temporary protection of the perimeter of the regime object. The majority of cyberattacks originate from mobile devices, and the prevalence of wireless communication methods inside the system provides ideal circumstances for a successful cyberattack. It has been shown that entry points (access) into the corporate network are the most common way that hackers gain unauthorised access to the network or utilise the network to conduct a distributed denial of service attack [4, 5, 6, 10, 11, 12]. The usage of wireless networks, cloud services, etc. does not offer a reliable perimeter of cybersecurity of the object due to the huge number of sensors linked to the system. The unauthorised disclosure of sensitive user information is another problem (companies). The machine learning and AI technologies used to combat cyber threats serve a dual role, yet both are necessary due to the severity of the problem (the algorithms used can both counteract cyber-attacks and create them). There are always going to be new cyber risks, and the only way to combat them is to deploy cutting-edge information technology.

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,

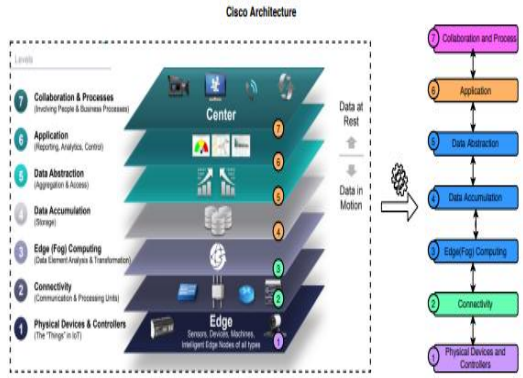

Figure 2: Cisco IoT Architecture

• 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

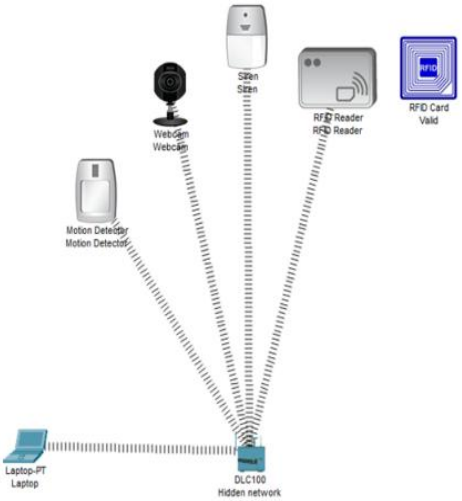

Figure 3: Cluster protection zone

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)

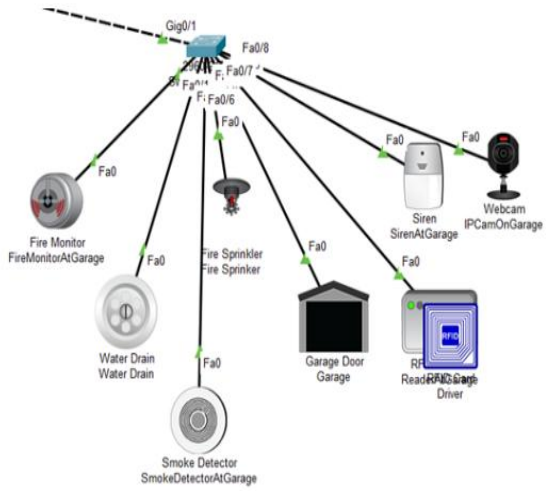

Figure 4: Scheme of fire alarm system of a separate room on the example of a garage

- 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:

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

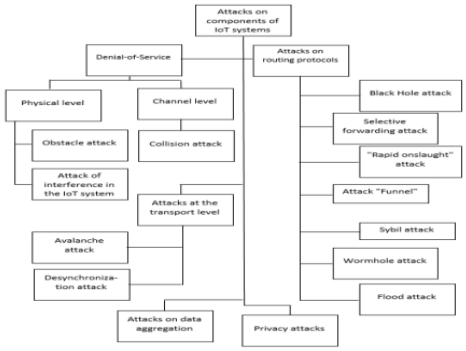

Figure 5: Attacks on IoT system components

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.