Cyber Security for IoT Research Paper

Emma C., Ethan C., Joshua S., Adarsh C.

July-August 2025

Abstract

This study was conducted to investigate the vulnerabilities of IoT devices, such as cameras, smart watches, and baby monitors. Due to limited resources, a physical demonstration wasn't possible; however, through the use of articles and other published works, past incidents, current security improvements, and the impact of AI were studied. Devices without updated software, multi-factor authentication, and weak passwords were the most susceptible to attacks. Nonetheless, devices with these features could still be compromised through holes in their code and DDoS attacks. Humans have become increasingly reliant on IoT devices; as a result, they should be aware of potential risks and actions that can be taken to minimize these threats.

1 Introduction

What if the devices designed to simplify your life end up compromising your privacy? A smart TV might double as a surveillance tool, a fitness tracker could expose your personal health information, and a connected car might be remotely taken over. These vulnerabilities show that helpful technology made for everyday use can quickly become a threat.

The Internet of Things (IoT) refers to physical devices, vehicles, or objects that contain software and can connect to the Internet. These "smart objects" range from home devices like thermostats and light bulbs to industrial machinery and vehicles. By utilizing these devices to optimize various aspects, human life can become more efficient. For example, companies use IoT sensors to monitor equipment performance and detect potential problems before they cause any trouble. [1]

The rise of smartphone technology has allowed many devices to become part of IoTs and has increased the number of connections. However, this surge in connected devices also brings more security challenges. Many IoT devices are vulnerable to hackers and other cyber-attacks, which puts data at risk. Furthermore, when user signals are intercepted, the privacy of individuals can be compromised, giving access to personal information. [2]

Common security protocols that IoT devices use are encryption methods like TLS (Transport Layer Security) to protect data in transit, and authentication

protocols to verify device identities. Some devices are designed with security in mind and have the appropriate security systems, such as encryption, authentication, and access controls. Similar to how Web protocols like HTTP enable data exchange on the Internet, IoT protocols offer these devices connected to the Internet a way to communicate more easily. [3]

2 Hacks Through History

In 2015, two researchers, Charlie Miller and Chris Valasek, performed a remote hack on Jeep Cherokees that could manipulate the car's windshield wipers, radio, and engine. This hack was possible due to a vulnerability in the car's infotainment system manufactured by Harman International. 1.4 million vehicles were affected, and as a result, a product recall was issued. Although this event led to Harman International making efforts to secure its products and mass changes in automotive cybersecurity, the complexity of modern vehicles continues to increase. As is evident, vulnerabilities in IoT devices can be detrimental to a company as a whole, leading to a loss in profit and possibly lawsuits.

Figure 1: *News Report of the Remote Jeep Hack*

Following this hack, a DDoS attack was launched on the Dyn service provider using an IoT botnet in October 2016. This hack led to many websites going down, including Twitter, The Guardian, and Netflix. This botnet was made possible through malware known as Mirai. Mirai uses computers to search the internet for defenseless IoT devices and then uses default credentials to log in and infect each device. Similar to biological viruses, Mirai malware variants have emerged and continue to threaten a wider range of IoT devices. This demonstrates that vulnerabilities in IoT devices can impact the internet as a whole, in addition to affecting individual devices.

Arguably, one of the most frightening hacks occurred in 2017 when the FDA

confirmed cardiac devices from St. Jude had many vulnerabilities. Hackers were able to exploit these vulnerabilities and interfere with a patient's heartbeat. To further explain, through the transmitters within these devices, hackers were able to drain the battery and cause malfunctions. Instead of personal data being at risk in this scenario, physical health and the life of a patient were at stake. The probability of these attacks increases as more medical appliances are connected to the internet. [4]

3 Physical Demonstration

Security cameras are often hacked due to poor user decisions or preventable vulnerabilities. As the attackers, we would've begun by checking the internet for these exposed devices by using tools like Shodan. Once we find our target, we would have looked for weak or default passwords, leaked credentials from data breaches, or intercepted footage from devices lacking encryption. Sometimes, access is given to hackers through insecure mobile devices that are linked to the camera app. [5]

Figure 2: *Example of a Home Security Camera Often Targeted by IoT-Based Hacks.*

After remotely compromising the camera, we would have demonstrated any indicators of a breach, such as camera malfunctions, unexpected movements, and suspicious notifications. It is important to note that some signs may be more indistinct, such as slightly slower network speeds, unfamiliar account logins, and

changes in privacy settings. Therefore, regularly investigating one's security systems is equally important as heeding blatant warnings.

After determining that the camera had been hacked, we would've taken the necessary measures. First, we would have disconnected the camera from the internet to interrupt the hacker's remote access. Next, all the passwords would have been changed to prevent future hacks. Then, the camera's firmware would've been updated to avert hackers from exploiting outdated software. The demonstration would have concluded with a security audit that identifies all connected devices on a specific network to check for unfamiliar users. [6]

4 The Benefits of AI in IoT

Technology is advancing rapidly, and AI is changing the way we protect ourselves when online, especially with Internet of Things (IoT) devices. These devices are always on, often difficult to secure, and incredibly vulnerable to hackers. AI is working to enhance cybersecurity by analyzing the vast amounts of data generated by IoT devices and identifying patterns that indicate potential threats in ways that humans cannot.

This is achieved through a process called machine learning. AI learns through the data generated from IoT devices, including usage, sensor data, and communications, and builds knowledge of strange behavior and potential risks over time, much like a person learns from experience. Eventually, AI recognizes what "normal" is without having a list of potential risks to consider. [7]

For example, smart homes have AI monitoring devices such as alarm systems, smart locks, cameras, and voice assistants. If something out of the ordinary happens, like a security camera that sends video to an unknown location, the AI will recognize the activity and alert the homeowner. Connected cars use AI to detect hacking attempts that might compromise safety features. In healthcare, AI protects sensitive data by defending against attacks on wearable devices and hospital systems.

The world is becoming more connected, with more IoT devices and more entry points that have vulnerable attack surfaces. Artificial intelligence (AI) will be an essential part of protecting these devices against those vulnerabilities. AI can identify patterns within data, detect anomalies, and provide real-time information.

5 The Challenges of AI in IoT

Although AI can be a very beneficial tool for many fields, such as cybersecurity, if AI were to be placed in the wrong hands, it could cause serious damage and many problems. Some of these problems are the creation of sophisticated malware. This malware can be spread throughout a network, essentially creating botnets from IoT devices that can be used for DDoS attacks, or to gain information about vulnerabilities and weaknesses that can be abused, to compromise, or

steal data. Additionally, since AI is constantly evolving and advancing, features such as AI voice imitations are also improving, leading to bypassing biometric security measures in smart devices and breaching unauthorized access points. [8]

6 Practices to Secure IoT Devices

- **Continuously update software/software**, manually or automatically. Updated softwares/software allows the device to have the latest patches and bug fixes, reducing vulnerabilities. [9]
- **Implement MFA** (*Multi-factor authentications*). MFA greatly reduces device and account breaching/control from attackers. MFA requires multiple forms of authentication to access the device, such as biometric features (*fingerprints, Face ID, etc.*) and verification features, which revolve around what the original user "has" (*Authenticator app, SMS code, etc*). These features reduce successful attacks by attackers, strengthen security, and protect data privacy. [10]
- **Change default passwords/settings**. Smart devices tend to come with default settings that are designed to be user-friendly but very insecure.
- **Implement strong passwords**. Strong passwords are a crucial step in protecting your data. Use passwords that are 8-12 characters with at least 1 uppercase, 1 lowercase, 1 number, and a special character to have a good password. [11]

References

[1] IBM. What is the internet of things (iot)?, 2025.

[2] Eyal Katz. Top 5 most commonly used iot protocols and their security issues, June 4 2024.

[3] Fadele Ayotunde Alaba, Mazliza Othman, Ibrahim Abaker Targio Hashem, and Faiz Alotaibi. Internet of things security: A survey. *Journal of Network and Computer Applications*, 2017. ScienceDirect article ID S1084804517301455.

[4] IoT For All. The 5 worst examples of iot hacking and vulnerabilities in recorded history, 2025. Accessed: 2025-08-01.

[5] Security.org. Can home security systems be hacked?, 2025. Accessed: 2025-08-03.

[6] Pro-Vigil. How to tell if your security camera has been hacked, 2025. Accessed: August 3, 2025.

[7] PTC. Using ai to enhance iot security, 2021. Accessed: 2025-08-04.

[8] Insights2TechInfo. The rise of ai-powered attacks on iot devices, 2023. Accessed: 2025-08-04.

[9] Consumer Reports. How smart appliances could expose you to hacking risks, 2024. Accessed: 2025-08-04.

[10] IoT For All. Multi-factor authentication is crucial for iot security, 2025. Accessed: 2025-08-04.

[11] Cybersecurity and Infrastructure Security Agency (CISA). Good security habits, 2019. Revised June 14, 2019; accessed August 4, 2025.