# The Potential Security and Privacy Threats with the Internet of Things

David Ahlstrom

George Mason University

IT 104-DL2: Introduction to Computing

September 10, 2021

George Mason Honor Code

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on https://oai.gmu.edu/mason-honor-code/ and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material 2 copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://copyright.gmu.edu/?page_id=301 web site."

## Introduction

The internet of things, commonly shortened “IoT”, is the way to define the growing connectivity between various devices that can access the internet. Some examples of these devices are smart phones, smart watches, cameras, or even home appliances. These devices are harnessed to collect data, generally leading to the creation of new services for users and industries. This collection of data can lead to new advancements in technology by helping engineers and developers get a better grasp of how and why we use these devices. The IoT also allows us to be more connected than ever before. While this connectivity can lead to further advancements in technology, the IoT also poses security and privacy issues for users. The primary security issue with the IoT is confidential and personal data being compromised by cyber hackers. Also, because the IoT connects a plethora of devices, ranging from smart watches to power grids, attacks on IoT systems tend to affect the entirety of the devices, rather than just one user.

## Current Use of IoT Devices

There is a wide variety of applications for devices that are connected to the IoT. One example would be for public safety while driving. Roadside sensors, such as wireless MacID readers, are deployed in highways and various high traffic roads to measure the speed of traffic via tracking the drivers’ mobile phones (Georgakopoulos & Jayaraman, 2016). One of the more popular devices in the IoT ecosystem are wearables, most common being smart watches. These devices can monitor your vitals and can offer personalized monitoring for improving fitness (Georgakopoulos & Jayaraman, 2016). Another usage case with the IoT is in healthcare. Doctors can use devices to monitor patients in rural areas remotely while residing in big cities (Noida,

2019). There is an unbelievable amount of uses that arises from the IoT, and everyday companies form new processes for collecting and using data for certain tasks.

The Internet of Things is also implemented in the food industry, specifically in food safety technology. Emerson Electric, an American multinational corporation located in Missouri, provides engineering services for a wide range of markets. The *Mean Report* published an article describing the use of IoT in food safety, by discussing how Emerson is using real-time monitoring of food throughout the food cold chain, which is an interconnected system of facilities and vehicles that are designed to preserve food safety (Mena Report 2016). Emerson uses small, IoT connected sensors to monitor the temperature of the foods being transported (Mean Report 2016). This is yet another example of how the IoT is used as a great benefit in our society by keeping food safe to consume, even throughout the journey of farm to plate.

## Security & Potential Risks with IoT Devices

Devices connected to the internet of things are primary targets for cyber attackers due to their ability to collect important and crucial information. Securing IoT devices is critical to keeping the users and the companies safe from threats. One example is in the health care industry, where IoT devices such as pacemakers and glucose monitors are capable of being hijacked. “According to the results of Vectra Network’s quarterly post intrusion analysis report, in the first quarter of 2017, healthcare was the most targeted sector for cyberattacks” (Djenna et. al 2021). Consequences are massive for hijacked IoT healthcare services devices and can lead to these devices either malfunctioning or even shutting down (Djenna et. al 2021). Adept security measures for IoT devices are of utmost importance to not only the companies providing these devices and services, but more importantly the users and their information or uses of these devices.

In 2015, Chrysler was the victim of a massive cyber-attack. This was a different sort of cyber-attack, as it was planned in an effort to test the capabilities of the car's network security systems. Two network engineers, Charlie Miller and Chris Valasek, used a standard internet connected computer to hijack the systems of a Chrysler Jeep Cherokee driving down a highway in St Louis, and were able to activate the windshield wipers, turn the radio and air conditioning on maximum, and disengaged the car's transmission to make the vehicle undriveable (Bray, 2015). This security breach resulted in over one million Chrysler vehicles being recalled and stands as a warning to car manufacturers and drivers that these breaches are very possible on IoT connected vehicle systems. Kathleen Fisher, a computer science professor at Tufts University commented on this security breach stating: "Automotive computer networks are inherently weak and difficult to secure" (Bray, 2015). This is yet another example of how ultra-connected systems such as the internet of things leads to disastrous security threats.

## Ethical & Social Implications of IoT

The main ethical concern of the internet of things is the privacy of the users. With devices collecting data about your personality, shopping habits, physical well-being, and much more, the question is if this is ethical. Scott Peppet of the Texas Law Review also discusses the importance of consent with IoT connected devices. "Consumer consent offers one way to reconcile these competing realities: if consumers understand and consent to the data flows generated by their Fitbits, car monitors, smart home devices, and smartphones, perhaps there is no reason to worry" (Peppet 2014). The problem with consumer consent is that many times the devices used to track data are often small, screenless, and offer no input or output (Peppet 2014). For this reason, users may not even understand the terms and conditions of these devices, and

how they are using their data. Offering users a privacy policy or a terms and conditions page is crucial for those that don't want their personal data shared with companies.

"A study from Hewlett-Packard found that 90 percent of connected devices are collecting personal information, and 70 percent of them are transmitting data without encryption" ("One Year Later", 2015). This is a harrowing statistic and reminds us that our personal information is constantly being collected and transmitted to the companies who manufacture these IoT devices. These ethical questions are also directly tired with the potential security risks of the IoT, as many of these devices are designed with usability and not security in mind. They are often cheap to manufacture as well. It is important that the general public who own and operate these IoT connected devices are educated on the data sharing that occurs when using this technology.

## The Future of IoT

The internet of things is advancing incredibly quickly, and we are already seeing new systems in place that we didn't see only a few years ago. One example of the internet of things moving into the future are smart cities. Smart cities encompass cars, homes, offices, parking lots, and everything else that a city contains (Sultan 2017). Through the use of IoT devices, such as sensors and lights, this data being collected can improve infrastructure and public utilities. An example of IoT being implemented in offices is each individual would post their schedule, and depending on what office they are assigned, different rooms or offices could be lowered or raised in temperature, leading to less energy consumption. The only foreseeable future in IoT is even more connectivity, and with more connectivity comes more technological advancement, increased quality of life, but also security and privacy threats. As the IoT grows, I hypothesize that we will see more possible government intervention on the data transmission that occurs in these devices in order to further protect the general public from cyber-hackers. Hopefully, as

these devices and connected systems become more advanced, so do the security measures implemented to keep the users safe.

The future of IoT could also involve a popular advancement in the information technology field, artificial intelligence. Artificial intelligence, or AI, systems are implemented on a large scale in businesses to increase the efficiency of whatever computational process is occurring. These systems learn from previous mistakes and can perform tasks that previously may have required a human to perform. In the book, *Internet of Things: Integration and Security Challenges*, S. Velliangiri and colleagues discuss how AI and machine learning play a role in protecting the networks of IoT devices, specifically in the healthcare field. "The process of profiling devices, capturing network information, and identifying threats are all necessary steps that require AI/ML to cope with modern network conditions and continuously evolving malware" (Velliangiri et al., 2021). Not only can these AI programs lessen the workload of humans operating computer systems, but they can also be much quicker at discovering and solving security issues. Much of the future of IoT includes various other emerging technologies in the information technology field.

## Conclusion

The internet of things is becoming rapidly more commonplace in our society, and it is up to the designers, the users, and even governments to ensure that it is being used for our best interest. The increased efficiency and connectivity of these devices allows us to communicate with each other and optimize our daily lives. Smart watches can keep us fit, and smart cities can lead to better energy efficiency and a cleaner environment. The security and privacy concerns should certainly be understood and talked about in order to protect users. It's important that individuals understand which devices are IoT connected, and how to protect yourself from cyber

threats. While some may believe that the IoT is a net negative for society, the possibilities are endless when devices are connected to each other at such a large scale.

## References

Bray, H. (2015, Aug 03). After car hack, Internet of Things looks riskier: In a connected world, calls for more security. Boston Globe http://mutex.gmu.edu/login?url=https://www-proquest-com.mutex.gmu.edu/newspapers/after-car-hack-internet-things-looks-riskier/docview/1700594765/se-2?accountid=14541

Bray's Boston Globe news article describes the planned security test of the Chrysler automobile's IoT system. She talks about the threat the IoT poses to automobiles. She also talks to various experts in the technology field and how security measures could be implemented to keep drivers safe from these attacks. This article is great for specific examples of how the IoT allows cyber attacks to become disastrous, due to the interconnected nature of these devices. Bray asks very legitimate questions and describes the potential chaos of IoT cyber attacks. I consider this article to be reliable as Bray documents the Chrysler car hack situation and elaborates on the future of these IoT connected car systems, and their potential security risks.

Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure. Applied Sciences, 11(10), 4580. http://dx.doi.org.mutex.gmu.edu/10.3390/app11104580

This brief academic journal article by Djenna and colleagues discusses the potential cyber threats in the IoT ecosystem. the authors describe the main vulnerabilities in the IoT infrastructure and describe the potential strategies to avoid these devastating situations. They provide statistics of estimated connected devices, and the history of cyber attacks. They also discuss the smart health and IoT health industry, which is a major subset of IoT as a whole. Overall, the article presents a serious concern and describes why it is

important to stop these threats. This article is reliable as it presents empirical data on the IoT health-care industry and describes the security concerns of this technology in these spaces.

Georgakopoulos, D., & Jayaraman, P. P. (2016). Internet of things: from internet scale sensing to smart services. Computing.Archives for Informatics and Numerical Computation, 98(10), 1041-1058. http://dx.doi.org.mutex.gmu.edu/10.1007/s00607-016-0510-0

Jayaraman and Georgakopoulos' "Internet of things: from internet scale sensing to smart services" could best be described as a crash course in IoT. They describe its uses, applications, and potential issues. They also go more in depth on how IoT devices collect data and how these companies are using this data. They also define Semantic sensor networks, or SSN, and how these systems are used to define and discover IoT devices and their data. I was able to learn the basics of IoT as well as specific applications. With specific applications presented by the authors in this article, they are able to describe my research topic in a broad sense. This was a very reliable source of information for my research.

Internet of things: Technology, use cases and the challenges. Communications Today. 2019. http://mutex.gmu.edu/login?url=https://www-proquest-com.mutex.gmu.edu/trade-journals/internet-things-technology-use-cases-challenges/docview/2183237802/se-2?accountid=14541.

The Communications Today article discusses the uses and challenges posed by the IoT. Healthcare is discussed, and how the IoT leads to more efficient treatment of patients, allowing doctors to remotely monitor patients. The automotive sector is also discussed, and how the IoT allows sensors and tracking devices lead to a safer driving experience.

Security is also discussed, specifically how because the IoT is a widely connected network, the entirety of the network could be at risk if one of the devices is breached. The author or authors, as there is no listed author, end the article with the statement that security is paramount to the IoT. This article is reliable for my research as it provided more specific examples of IoT security issues and the challenges manufacturers and users face with this technology.

Liu, Y., & Chou, Y. J. (2018). Big data, the Internet of things, and the interconnected society. Telecommunications Policy, 42(4), 277. http://mutex.gmu.edu/login?url=https://www-proquest-com.mutex.gmu.edu/scholarly-journals/big-data-internet-things-interconnected-society/docview/2088799585/se-2?accountid=14541

Yu-li and colleagues scholarly journal article poses a question about the trustworthiness of IoT. Data collection and privacy is a big issue amongst users as well as governments. They describe how "big data" and IoT are essential components of an interconnected society, and how they could lead to reduced trust in the online environment. The authors give benefits as well as ethical risks involving IoT and data collection. This brief journal article raised similar concerns I have with IoT, how these companies plan to collect and use individuals' data. This article is certainly reliable as it discusses the legal and ethical issues of IoT and data sharing, with specific, cited examples.

One Year Later: Privacy and Data Security in a World of Big Data, the Internet of Things, and Global Data Flows. (2015, Mar 10). Targeted News Service http://mutex.gmu.edu/login?url=https://www-proquest-com.mutex.gmu.edu/wire-feeds/one-year-later-privacy-data-security-world-big/docview/1663410938/se-2?accountid=14541

This article primarily discusses the ethical implications of big data and the IoT. They talk about how the federal government, specifically the Obama administration, took efforts to protect individuals privacy in the IoT era. They also talk about how the data collected from IoT devices does have benefits, specifically in the healthcare and transportation industry. They ask important questions and state that these companies are not designing these IoT devices with security in mind, rather usability. They also talk about the "Consumer Privacy Bill of Rights" and how this might need to be implemented in the IoT connected world.

Peppet, S. R. (2014). Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. Texas Law Review, 93(1), 85-176. http://mutex.gmu.edu/login?url=https://www-proquest-com.mutex.gmu.edu/scholarly-journals/regulating-internet-things-first-steps-toward/docview/1636877419/se-2?accountid=14541

Scott Peppet's "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent" is a deeper dive into the issue of privacy in the IoT ecosystem. He describes how these companies tend to slip around offering explicit consent forms. He also talks about government policy that is mandated to prevent privacy intrusion. The most interesting aspect of Peppet's article for me is how some IoT devices are unable to offer information on how they collect and process user data. This can lead to users being blind to the fact that their actions are being tracked and used by companies. The ambiguity of these devices is a bit harrowing, and can lead to further privacy intrusions. Scott Peppet's article is very reliable, and was crucial to my research

on the legal and ethical issues of IoT. This article was extensive, and provided copious examples and sources and data sharing.

Sion, G. (2019). Smart City Big Data Analytics: Urban Technological Innovations and the Cognitive Internet of Things. Geopolitics, History and International Relations, 11(2), 69-75. http://dx.doi.org.mutex.gmu.edu/10.22381/GHIR112201910

Sion gives specific examples of IoT being implemented in the form of smart cities. He collected data from thousands of respondents in order to formulate the results. He gives empirical evidence of a few examples, such as how smart cities can reduce the cost of living. He also discusses how cities fund IoT infrastructure. I was able to learn through evidence and numbers of IoT is shaping our cities. Although this article was listed without an author, I believe it is a reliable source due to the specific, cited examples listed and discussed in the article.

Sultan, H. (2017). Internet of Things: Future of Cloud Computing. International Journal of Advanced Research in Computer Science, 8(2) http://mutex.gmu.edu/login?url=https://www-proquest-com.mutex.gmu.edu/scholarly-journals/internet-things-future-cloud-computing/docview/1901445075/se-2?accountid=14541

Sultan offers a brief history of IoT and estimates what it will look like in the future. Some examples of what he believes is the future of IoT are effective electricity generation, smart cities, and revolutionizing retail markets. We can see some of these implanted today. He also offers concerns primarily surrounding the security aspects of IoT. Sultan believes that IoT is the “next big thing” we would see in the world, and I would argue that it is the “current big thing”. I consider Sultan’s article to be reliable as he discusses

the documented history of IoT and hypothesizes the future of this technology. He offers current uses of IoT and elaborates more so on the future.

United states : Emerson uses internet of things to enhance cold chain leadership, help safeguard food safety. (2016). MENA Report, Retrieved from http://mutex.gmu.edu/login?url=https://www-proquest-com.mutex.gmu.edu/trade-journals/united-states-emerson-uses-internet-things/docview/1840598250/se-2?accountid=14541

This brief business news source article published by the *Mena Report* provides yet another example of IoT being implemented in various fields. The food safety industry is discussed, and how a corporation called Emerson is using small IoT connected sensors to track the temperature of transported food in order to maintain the safety of consumption. The article also describes how consumers are concerned about food safety, and that these devices can help protect the consumers. This article is reliable because they are simply stating news and not providing any personal opinion on the matter. Statistics and examples are provided, which allowed me to gain further knowledge on how IoT is implemented in our world. My research was greatly enhanced by this article.

Velliangiri, S., Kumar, S. A. P., & Karthikeyan, P. (2021). Internet of things: integration and security challenges (First edition.). CRC Press/Taylor and Francis Group, LLC.

Velliangiri and colleagues' book contains a vast amount of information regarding the history of IoT, blockchain, and security measures implemented in IoT spaces. They discuss how different security measures, such as AI integration, blockchain integration, and cryptography integration in IoT are all potential positives in increasing security and data privacy. I didn't read the entirety of the book, but to briefly summarize the chapter in

which I did read, where the authors discussed the integration of AI in IoT security systems, Velliangiri and colleagues described how these AI systems are coded and taught to protect IoT devices. Through machine learning, these AI systems capture and process data in order to determine if this data is safe to collect and share. This book is a reliable source of information for my research as they provided copious citations and resources used to write this book.