The Internet of Things (IoT): Its Risks and Benefits

Courtney C. Riojas

Blue Ridge Community College

Author Note

This paper is prepared for English 110, taught by Professor Karyn E. Fisher.

Abstract

The Internet of Things (IoT) has become increasingly more prevalent since it was first introduced and has created many benefits that businesses and individuals use to make more intelligent decisions and a much easier life. With this sudden increase in devices connected to the Internet, there has also been an increased risk that the information these devices gather, store, and transmit can be hacked into, stolen, and used for purposes not initially intended. Given the security risk they introduce, the risk of using IoT might be greater than the benefits they provide at this present time.

Keywords: IoT, Internet of Things, security risks, personal information, data collection, hackers

The Internet of Things (IoT): Its Risks and Benefits

Since the introduction of the Internet of Things (IoT), devices that are connected to each other and the Internet, they have immediately been implemented for multitudes purposes that extend from entertainment to making work easier. With this advancement in technology, there have come along risks which users and developers have been made aware of through their use. These issues have caused developers to figure out ways that they can improve the security of these devices so that they can continue to be used with confidence. This paper will cover the benefits that IoT brings, the risks that are involved in using these devices, and whether the risks outweigh the benefits.

How Are They Used to Benefit Us?

The Internet of Things (IoT) are devices connected in some way to the Internet and can be used to benefit both businesses and individuals. Dyness (2018) describes the rewards this technology brings to businesses, of which the following are just a few:

- making data collection and feedback on products more attainable to anyone,
- making workplaces safer and more efficient,
- figuring out trends in customer's purchases and use of products,
- and providing data with which more informed, intelligent decisions can be made, thus increasing sales and efficiency (pp. 50-51).

With data being collected, automatically organized, and displayed, it is easier to see trends, find where things are weak, and act on the information provided. IoT allows remote access to certain processes and automated them, eliminating a lot of errors due to forgetfulness and freeing individuals to turn to other tasks. Some of the uses have been beneficial for agriculture, for example, because it eases the time and energy farmers take to monitor and care for their animals remotely, allows them to tend the crops more efficiently by analyzing the contents of the soil and recommending when to add more additives, and eventually will free farmers from having to manually drive tractors in their fields (*"*The Next Step in Innovation,*"* 2017, p. 20*)*. These advances free farmers to do other activities around the farm, decrease the amount of physical labor on their bodies, and allow them to see what is happening as it occurs. Another way it is implemented is with air systems. IoT systems can be used to monitor the air quality of buildings, analyze what the air contains, and anticipate potential issues with the system, notifying the proper people to address them (Siegel, 2019, p. 24-26). For businesses, the automation of mundane tasks has created ease, and the data collected from it allows for more intelligent decisions on practices and products.

The more prevalent use of IoT is among individuals in their own homes and lives. The more common place examples are Alexa, Google Assistant, and Siri which with their voice-activation allow people to quickly do Internet searches, control other IoT-connected parts of their house, play music, and much more. For example, in the middle of a conversation when an uncommon word is used, someone can quickly "wake up" the assistant and ask for the unknown word to be defined. The assistant will then search for the word and define it. Besides Internet assistants, there are IoT toys which can be interacted with via phone apps, laundry machines that can automate the entire washing and drying process, security cameras that can send images to your mobile device when you are away or when something unexpected happens, and even toothbrushes, like Ara produced by Kolibree (https://www.kolibree.com/en/) is one of them, that can be used to get feedback on how well teeth are being cleaned. There are multitudes of IoT devices which are changing life into what has been only imagined in science fiction. Where it will lead to will be a matter of great interest in the next few decades.

What are the Risks Presented to Us?

While all these benefits have advanced businesses and made life easier in some cases, IoT has introduced risks that, unless properly addressed, can critically harm the businesses and individuals who use them. Because so many devices are attached to the Internet with little to no security precautions in place, it means that these devices can be hacked and used by hackers to move into the network and other devices attached to it. Bridge (2017) brings up that in 2016, there was a bot net attack called Mirai which shut down websites on much of Europe and the US because it took advantage of the lack of security in many IoT devices whose passwords were the default ones provided by the manufacturer (p.4). Hackers can infiltrate these devices and use them to conduct DDoS (denial of service) attacks on other networks by bombarding them until the entire network comes to a halt. The consequences of this are many. With banking, for example, a DDoS attack could halt and cripple people and businesses who would be unable to access their financial assets, hurting the economy. Dixon (2017) brought up another, more serious effect, which would be a hacker infiltrating IoT-connected medical equipment and using it to end someone's life remotely, but he makes note that this threat has been addressed by the FDA by requiring wireless medical devices to pass particular security tests if it is to be used ("Remote Management and Monitoring of Patients and Medical Equipment"). However, there is always the chance there is a small gap in the security that a smart hacker can slip into and use to wreak havoc.

Another threat that IoT introduces is the matter of personal data collection. Because these devices are connected to the Internet and collect data, whether it be audio, video, or sensor readings, they are able to gather information that can be manipulated and abused if it falls into the hands of a hacker, stalker, identity thief, or dishonorable data collectors. There have been instances where IoTs have been used to gather preferences of individuals and use them to promote certain products that the person would be interested in. The data collected could also contain important information such as birth dates, social security numbers, health issues, and other sensitive information that could be stolen and used to cause great harm, if hacked into. For example, there was an IoT teddy bear that got hacked and allowed the hackers to see sensitive information about the child (Davies, 2016, p. 61). Because of the amount of data that gets collected by IoT devices, it makes it essential for them to be secure; however many of these devices have been built leaving out this important feature because the manufacturers never saw them to be necessary. Robinson (2015) notices:

> The simplest device, a lowly toaster, for example, can become an entry point for an industrious hacker to use shared network resources in the benign environment of a home to access corporate assets that the homeowner taps into. And the world at large is almost wholly unprepared. Indeed, most IoT devices have not been built with security in mind...The companies that make the devices haven’t thought of themselves as information or data companies either. Yet, that is what their products do: gather information and transmit it over the internet to servers or systems located somewhere else - and possibly under the care of another organization. So they’ve not taken steps to protect their devices the way, say, a smartphone maker might (pp. 20-21).

Therefore, it is imperative that companies who make IoT devices to design them so that there are security measures in place to protect vital information from hackers. Yanamalda (2015) suggested that manufacturers begin to design from the start so that their devices to have security throughout instead of adding it in later (p. 32).

Finally, one of the threats that these devices produce is that they can be used to surveil individuals. This is most obvious with Amazon's Alexa which has had multiple cases where there have been eavesdropping or has accidentally woken up and recorded conversations or incidents that it should not have heard. Knowles (2020) states that:

> Last year Amazon admitted that staff and contractors listen to and transcribe random snippets of people's conversations with Alexa to make sure it is responding to commands efficiently. The recordings include instances in which Alexa was triggered by reacting to an incorrect "wake" word. The resulting recordings have included information such as bank details and what may have been sexual assault. Dave Limp, of Amazon, told the programme, broadcast last night, that workers listened to less than 1 per cent of conversations, which were anonymised, and that an opt-out option was now offered (p. 9).

Although the results are made anonymous and individuals can choose to not be involved in letting their audio be listened to, does this stop companies from using the information or sharing it with other entities even if the individual opts out of it? What if someone were to use it to do surveillance of individuals? Worse still would be if a malevolent government decided to use it to listen in to people's conversations? These are things that need to be looked at when considering these devices, and for companies who are involved in IoT to practice integrity with.

Risks vs. Benefits: What Do You Do?

The increased use and prevalence of IoT devices has increased the awareness of the need for better security and handling of personal information and data. Because of this, there are companies and individuals who are working on improving IoT devices so that they are more secure. These are good and necessary developments if society is going to use them more. One need asks though, if having Internet-connected devices are essential? Do we really need an Internet-connected toothbrush, for example? Does it improve our life more than a regular one? By increasing automation of tasks, will we increase our dependence on them and eventually no longer know how to make the decisions or do the tasks on our own? There is more to this world than what can be picked up on sensors, and even the sensors can be tricked or tampered with. Will we know what to do should the Internet give out? Will we decide to trade our own privacy and information for the sake of convenience? Is the data that we have allowed the IoT devices to collect our own or is it no longer ours? Are there other ways for devices to be automated and to collect and process data that would guarantee the security of it all? These are all questions that should be considered. The benefits and applications of IoT are many and make life more convenient; however, until the issues of privacy, usage of collected data, and security are addressed, caution must be taken when implementing these devices in our homes and businesses. Questions must always be asked, and the risks weighed against the benefits.

References

Dixon Jr., J. H. B. (2017). The Wonderful and Scary Internet of Things! *Judges' Journal*, *56*(3), 36–38.

Dyess, N. (2018). Top six benefits of the IoT: There are many benefits to implementing an Internet of Things (IoT) solution to maximize productivity and enhance an organization's workflow. *Control Engineering*, *65*(7), 50–51.

Emily Davies. (2016, February 24). Now fraudsters can hack your child's teddy. *Daily Mail*, 61.

Mark Bridge. (2017). Student gamers behind cyberattack. *Times, The (United Kingdom)*, 4.

Robinson, T. (2015). Appliance Takeover? *SC Magazine: For IT Security Professionals (15476693)*, *26*(10), 18–23.

Siegel, J. J. (2019). The Next Step in Innovation. *Engineered Systems*, *36*(3), 24–26.

Tom Knowles. (2020). I switch off Alexa for privacy, admits former Amazon boss. *Times, The (United Kingdom)*, 9.

3 Ways the IoT Revolutionizes Farming: Farmers use high-tech agriculture techniques to improve production output, and exploit sensors and other IoT technologies to create a more efficient operation. (2017). Electronic Design, 65(9), 12.