The Role Privacy Plays in the Greater Sociotechnical System of the Internet of Things

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Jiafu Li

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Bryn E. Seabrook, Department of Engineering and Society

Introduction

Imagine a scenario where a working adult opens the door to their house, and the lights turn on automatically, followed by the heating or air conditioning, and finally the television. Such an ideal system where each device knows how and when to operate itself can be achieved by something called the Internet of Things (IoT). IoT allows for different machines to interact with one another via sensors. In the scenario mentioned above, when the owner of the house returns home at night, the door sends a signal to all the other machines. Upon receiving the signals, the lights, AC, and TV each performs certain actions. Currently, Wi-Fi and Bluetooth have been some of the biggest communication network used by IoT systems. However, each of these functions have its disadvantages ranging from shortness of range, high power consumption, and high latency. Furthermore, IoT encourages peer to peer connections between machines and puts less emphasis on human involvement. The system should be able to function properly without monitors, thus the issue of security is a paramount concern for IoT. Without human monitoring, it is hard to tell if a data breach has occurred, and the machine's own security might not be enough to prevent data leakage. In this prospectus, there will be a technical project where I will discuss how using optical communication can better improve communications between devices and a sociotechnical analysis on how privacy plays a role in the greater sociotechnical system of the Internet of Things.

Technical Discussion

The proposed technical project discusses research with the UVA department of electrical engineering where we explored a new form of communication between the devices within the

IoT system. There already exist many great options such as Wi-Fi and Bluetooth, however, Wi-Fi suffers from low transmission rate, and Bluetooth suffers from short connection range. Optical Communication is a good alternative because light is easily accessible and can travel far distances in a short span of time. In order to test the functionality and real-life application of optical communication, a small model is constructed. Arduino is ideal for its open-source libraries as well as its easiness in implementing sensors. The Arduino Nano 33 IoT board is a small and effective board for sensors to be attached. IoT relies heavily on sensors for each device to communicate with one another, and Arduino provides easy interfacing between sensors and programming. The initial approach is to simply set up a peer-to-peer connection between one transmitter and one receiver. The transmitter will be programmed in such a way that it sends a signal at 38kHz frequency, because that is the frequency needed to emit an infrared beam. The data relating to distance traveled and clarity of the signals are recorded and analyzed so it may be used later when moving into multi-sensor communications. Optical Communication will allow for better and longer communication between devices that can overtake Bluetooth and Wi-Fi.

STS Discussion

IoT acts similar to a Smart City where data is transmitted electronically and problems are solved in real time. This form of data gathering and data processing is the desired future of a world full of technologies. IoT encourages human-less interventions; the idea is that all devices within the IoT system should be able to communicate with one another using sensors. The concept of machine-to-machine (M2M) interaction is heavily emphasized (Mehta et al.). Transmissions and receiving of data should be automatic and devices should always be on standby when new data arrives.

The British scientist Kevin Ashton first came up with the term Internet of Things to describe a "sensors embedded system" (Ray). Before computers have the ability to gather information on its own, humans are the main sources of computers' data. Humans input data either through the push of a button, or taking pictures and scan it onto a device. However, humans also have many other things they must do for their own survival, and the amount of time they can offer to data collection is very limited. It would be difficult for humans to capture live data in the real world simply because there are other more important things that require their attention. Therefore, if computers have the ability to capture information on its own without the help of humans, they would be able to keep track of almost all information. Energy, waste, cost, health, climate, all of these concerns can be accounted for and used to improve the world.

The two main STS frameworks I will be using to analyze the issue of privacy is Technological Determinism and Risk Analysis. With growing technologies and more and more people having access to the Internet, there is simply too much data and information for one device to keep track. Having a system like IoT can easily transmit and receive a large quantity of data without needing human interventions. Humans now have to rely on the performances of the machines to deliver and process the data. In short, IoT can now change the way human's digital data is stored, which demonstrates how technology is shaping society development. In an essay titled "*Technological Determinism in American Culture*" written by Merritt Roe Smith, Smith discussed how technologies are designed to be able perform tasks better than humans. Smith states, "in the competition for world markets, industrial societies pressed hard to develop technological capacities that would give them an edge and, in the process, made the machine rather than the human condition the norm against which all else was measured" (Smith 29). Smith argues how the standards for machines are different than for humans because they can do

a much better job than humans. IoT is one such example; IoT drastically improves the way data can be collected. IoT's ability to capture data in real time improves efficiency and reliability of the data as well as achieving a much larger sample size. IoT has since changed the way information is collected and shared, and that will be the new norm of data collection in the future.

As machines become more and more automated, the risk of security increases. IoT requires little to no human intervention, and so when there is a data breach or loophole, humans will not be alerted right away. Although being automated, machines might not have the capability to defend itself against outside invasions, and if one machine is overtaken, it is easy to overtake the rest of the system because everything can be linked to one another in IoT. The question then becomes whether or not the data breach is an "acceptable" risk? Given how efficient the IoT is in collecting and managing the flow of data, does this one advantage outweigh the security disadvantage? Is the risk acceptable enough for people to still trust in IoT to handle personal data? In a paper titled *Defining Risk* written by Gabe Mythen, Mythen discusses the importance of risk identification and the recognition of these existing risk. Mythen states that every risk also comes with some "level of public knowledge" that recognizes such risk (Mythen 68). It is important for all participants that shares information via the IoT system to be aware that IoT is more vulnerable to cyber-attacks because there are no cyber security specialists on watch to ensure safety of the network. It is important to take consideration of the security regarding IoT because IoT will be the future of how data is recorded, transmitted, and received. IoT has already improved society and will only continue to grow as the world moves towards automation, and with automation comes with the question of how to automate defense.

Research Question and Methods

The question guiding this research is "what role does privacy play in the greater sociotechnical system of the Internet of Things?" In order to effectively answer this question, I will be looking through research papers and academic journals that discuss various ways to help improve security. One potential approach is to improve security of the individual machine itself, while another approach can include restricting user access using access control or time constraints (Su, 919). The best solution can be derived by considering all approaches and integrating all the positive aspects. Two keywords that I will be using to conduct my research is "IoT" and "security." While these two keywords might produce very broad results, the core remains that it is good to consider all forms of security protocols so I may pick out the ones that will be most useful.

Conclusion

The technical deliverable focuses on a new way to improve connection and communication between each node within the IoT system. The STS deliverable focuses on how privacy concerns for IoT given its nature of being an automated system with little to no human interventions. IoT is important because it will be the main form of communication and data collection in the future. IoT is what enables smart cities as technology continues to develop in society. I anticipate IoT will become the norm similar to how the internet has already overtaken many people's lives. As IoT continues to scale, the individual security protocols of the machines must also scale to keep up with modern cyber threats.

References

Mythen, G. (2004). Defining Risk. Ulrich Beck: A Critical Introduction to the Risk Society. (pp. 53-73). London, England. Sterling, Virginia. Pluto Press.

N. Su, "Internet of Things privacy security protection access control Research," *2022 IEEE 6th Information Technology and Mechatronics Engineering Conference (ITOEC)*, 2022, pp. 919-923, doi: 10.1109/ITOEC53115.2022.9734497.

Smith, M.R. (1994). Technological Determinism in American Culture. *Does Technology Drive History?: The Dilemma of Technological Determinism*. (pp. 1-17). Cambridge, Massachusetts. London, England. The MIT Press.

S. Ray et al., "A Survey Paper on Architecture of Internet of Things," 2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2018, pp. 908-913, doi: 10.1109/IEMCON.2018.8614931.

V. Mehta, P. Bansal, K. Mohit and P. Banerjee, "Empowering the Security for Iot-Based Communications in Smart City," 2018 International Conference on Automation and Computational Engineering (ICACE), 2018, pp. 57-60, doi: 10.1109/ICACE.2018.8686995.