Internet of Things Research Paper

Lucas Biegel

College of Engineering and Computing

George Mason University

IT 104-001: Introduction to Computing

Ankita Kalath

September 24, 2024

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on https://catalog.gmu.edu/policies/honor-code-system/ 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 2 text, any material 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 https://universitypolicy.gmu.edu/policies/responsible-use-of-computing/ web site."

Introduction

IoT Technology grew in popularity with the idea of the "smart home" where one would have a network of interconnected hardware devices from smartphones to security cameras to improve the overall experience of one's life, this idea eventually expanded beyond the household and into "smart cities" and beyond. This paper will explore the idea of the "Internet of Things" and the current uses of the technology as well as potential questions for research in the future. It will also discuss concerns about security as well as the ethical and social implications of utilizing IoT technology in modern society to determine if IoT technology is a likely future that may be coming sooner than expected.

Background

Most people already have experience with IoT technologies, Devices such as amazon's Alexa or Google's home are both examples of household IoT technology that functioned as "hubs" for an IoT network in your house. Things like digital clocks that can give you the weather or turn on your lights in the kitchen, and many more use cases. These same concepts can be expanded to work in many other cases, such as the aforementioned "smart city" where IoT technology can be used to improve the overall quality of life of large population centers. IoT technology is used in the military sector as well, streamlining and improving communication, logistics, and effectiveness. There are billions of these devices, such as cameras, sensors, RFIDs, smart phones, and other wearable technology that are all separately owned and deployed for their own purposes to intermix the daily lives of people with technology. (Georgakopoulos et al. 2016).

Potential Benefits

The benefits of an IoT network are mainly its ability to mesh every part of a system together for expanded interoperability and adaptability. For example, in a city where the traffic lights are connected to road traffic monitors can help to alleviate congestion by dynamically changing its timings or to allow first responders easier access to accidents by rerouting most of the traffic away from the incident. This idea can be expanded with smart vehicles that are able to route themselves and link with the other two devices to further maximize its capabilities and ease of use. But you do not need to go to the scale of a city to see the benefits of this technology. Imagine waking up and getting a readout of todays weather and headlines, then going to workout where you already have a program designed around your smart watch's health readings. IoT technology is extremely scalable and versatile, due to its nature as a network of specialized devices, it can theoretically accomplish anything.

Legal and Ethical Issues

Unfortunately, IoT Technology is also associated with massive privacy concerns, where people do not want their every move to be collected and processed for some companies to optimize advertising. However, while there is also something to be said about the efficacy of these kinds of monitoring methods in police work, when criminals can no longer hide under fake names and appearances, the risk of data leaks or even just insufficient anonymization processes are far too great to be taken lightly, "Researchers once bought web browsing history data of German citizens and paired it with publicly available information to reveal the online habits of individuals." (Dellinger, 2023). Companies are too relaxed with stripping the data collected of personally identifiable information, and too relaxed about who they are sharing this information with for it to make anyone feel safe about using IoT technology, which is one of the fundamental obstacles from getting a wider adoption of the tech. From an ethical standpoint, the endless data

harvesting is also a major detractor where the IoT begins to look less like a utopia, and more of a capitalist dystopia, “when Google bought Nest, a maker of connected thermostats, it has an opportunity to communicate with consumers through the devices, perhaps selling you ads for fire extinguishers if your house is on fire.” (Steeves, 2015).

Security Concerns

Security is possibly the largest concern with IoT technologies, when every part of your life is interconnected, a single compromised device can lead a nefarious actor through the network and onto every other device connected. There is also the aspect beyond a private home, where entire databases of consumer data collected from security cameras or other big data collections could be compromised and offer unprecedented access to people who should not have it. As stated by Shammar and Zahary (2020), “If cybersecurity is not well managed, the hackers will take advantage of the weaknesses and defects of IoT objects and then will distort data or disrupt systems through the global IoT network” (p. 41). Furthermore, simply the size of an IoT network can make it a daunting task to secure entirely, there will always be some kind of flaw that no one noticed before, so the focus falls from prevention to risk mitigation, where you are reacting to problems as they arise compared to proactively trying to completely seal the network. This may mitigate the scale of data breaches but limits the ability to prevent them altogether. The idea of cybersecurity regarding an IoT network is nebulous and complex and is something that has no concrete answers.

Social Problems

The main social problem to consider is the aforementioned privacy risk, when it comes to IoT, everyone is concerned about how this tech is any different from 24/7 surveillance. One of the current storms overtaking the tech industry is artificial intelligence, or AI, with seemingly

every company stumbling to make its own AI chatbot or integrate AI into their webpages somehow. AI fits nicely into IoT technology as, in a perfect world, would be able to control all the entire network far faster than a human could. But for an AI to function properly, it needs a lot of data, and companies like Google are already reaching around the user to collect its data, such as scanning the faces of people in your photos to find them through image recognition, or the many other ways they harvest personal information to deliver targeted advertising. (Herman, 2024). Another angle is that not everyone wants technology to be any more an essential part of their lives compared to how it already is, and for many, IoT networks are the furthest thing from a bright future.

Conclusion

IoT technology is only getting increasingly ubiquitous in everyday life and does not seem to be going away anytime soon. While there are benefits to be gained from the technology, the security and ethical concerns cannot be ignored. It is a fundamentally flawed system that has the potential to improve the daily life of every human on earth, but because of that expansive ability, makes it practically impossible to lock down securely, or regulate to ensure privacy. Research in the future can investigate new architectures and systems that may be able to alleviate one or both major risks, but as of right now, an IoT future is potentially one of overreaching corporate control.

References

Dellinger, A. J. (2023). *Meta's Smart Glasses Ignore Why Google Glass Failed: The mixed-reality wearable are stoking massive privacy, security, and ethical concerns*. The Newsweek/Daily Beast Company LLC.

*An overview of recent advancement of IoT technologies introduced by meta and apple, mixed reality devices that are supposed to integrate the digital with the real world seamlessly, however there are still numerous privacy, security, and ethical concerns. This source is useful for getting a look at current IoT developments and tech. It also provides some angles to the ethical problems with IoT devices.

Georgakopoulos, D., & Jayaraman, P. P. (2016). Internet of things: From internet scale sensing to smart services. *Computing*, *98*(10), 1041–1058. https://doi.org/10.1007/s00607-016-0510-0

*This source provided a simple and understandable description of IoT as well as the current scope of development. It also provided examples of usable IoT services and providers, giving even more paths to research down. This source provides real world examples to draw ideas from and make connections to. It is a versatile source that can fit many different headings in the paper.

Goumagias, N., Whalley, J., Dilaver, O., & Cunningham, J. (2021). Making sense of the internet of things: A critical review of internet of things definitions between 2005 and 2019. *Internet Research*, *31*(5), 1583–1610. https://doi.org/10.1108/intr-01-2020-0013

*This source might be the best out of all of them in terms of giving a good view of the progress of IoT. This paper provides a timeline of sorts to follow the development of IoT over time and how it has changed through the years. It is also the newest, and because of its topic, it is the best paper out of all the ones I found to giving a modern look at IoT and its applications in the current world. Due to its size, it is hard to get a specific section to incorporate in the text and therefore mainly used to get a personal understanding of the topic.

Herrman, J. (2024, May 20). Screen Time: What will Google's push into AI mean for the future of privacy? *New York,* http://mutex.gmu.edu/login?url=https://www.proquest.com/magazines/screen-time/docview/3057688662/se-2

*a real-world example of data scraping done by google from their IoT devices and search engine, shows the real-world threat of privacy concerns associated with IoT devices and technology. Has some good quotes centered around privacy risks that makes it an easy source to pick from. Also, it is new, so it contains up to date information about the topic.

Shammar, E. A., & Zahary, A. T. (2019). The internet of things (IOT): A survey of techniques, operating systems, and Trends. *Library Hi Tech*, *38*(1), 5–66. https://doi.org/10.1108/lht-12-2018-0200

*This source varies from the first by being a much more technical overview of how IoT devices work. It is also much more recent, providing a more up to date view of where IoT is today. It also states security risks associated with IoT, which is important for the paper's requirements. It

is a little old, but not egregiously so and highlights a solid understanding of the topic and contains accurate predictions of the future of the tech, making it dependable.

Steeves, R. (2015). Privacy & data security concerns in 2015, part 1: The Internet of Things. *Inside Counsel.Breaking News,* http://mutex.gmu.edu/login?url=https://www.proquest.com/trade-journals/privacy-amp-data-security-concerns-2015-part-1/docview/1651729646/se-2

*A focus on the security aspects of it all, useful to get the more security focused look at IoT technologies, a little bit of privacy concerns as well. It is the oldest so I might not be able to use its examples, but for general understanding I could use it. There are a few quotes that match up to modern understanding as well, so one of those might work in the paper itself.