The Rise of the Smart Home

By Justin Jo, ECE '18

Introduction

The *Internet of Things* saw its first official mention in 1999 during a presentation by Kevin Ashton. At the time, computers were in the process of evolving from simple machines into greater, connected devices. Ashton described computers in the 20th century as "brains without senses" (Gabbai, 2015). In the beginning of the 21st century, computers began to connect to their senses in the form of devices that gained Internet connectivity. Some notable emergences include smartphones and smartwatches, with recent developments such as home assistants like Amazon's Echo™ and Google Home™ . With the advent of these devices, the role of technology began to grow outside of pure computation and into our daily lives. The Internet of Things (IoT) was the next big thing throughout the 2000's, but it is now the current big thing. As IoT continues to grow, its impact will begin to show in both society and everyday life. One result of this growth is the success of the smart home.

Origin of the Smart Home

The smart home is a concept that originated in the early 1900s and has had recent success with advances in IoT. The core idea of the smart home is assistance in chores around the household. In the 1910's, the introduction of machines such as vacuum cleaners, food processors, and sewing machines marked the first emergence of technology in the household (Rothfeld, 2015). Since then, advancements in technology have allowed more and more devices to enter the home space; it is now typical for homes in developed countries to have washing machines, toasters, dishwashers, and other similar appliances.

As IoT began its trend in mass media, manufactures of these appliances have adopted the notion of embedded devices. From this trend, the modern smart home is born. Now, a smart home consists of wifi-capable devices that replace their analog counterparts. Refrigerators, light bulbs, and even rice cookers can be found with internal computers (Williams, 2016). These embedded computers serve as the "senses" of the house, allowing the house itself to become an IoT device. This has allowed for the rise of yet another advancement in technology: the personal assistant.

The Home Assistant

The current iteration of the smart home emphasizes the home assistant, intertwining advances in technology with human-computer interaction. At the time of this report, the two industry leaders currently battling for control of the market are Google and Amazon, with Google Home and the Echo, respectively. Both offer a similar core product: voice controllable speakers with full IoT compatibility. They both come with music streaming services, built in search engines, and the ability to process complex voice commands (WIRED, 2017). Although impressive, these features are only scratch the surface of what these devices are capable of. The true power of these personal assistant lies in their integration with IoT devices. With this capability, homeowners unlock the ability to talk to their house. Nest Labs™ tackles this with its product line, which features a "smart appliances" such as a thermostat, lights, and security cameras around the house. Smart devices like these can be programmed to only operate at their minimum amount necessary,

allowing users to reduce their energy consumption by up to 20% (Jacobsson, Boldt and Carlsson, 2016). Other companies that take advantage of the current iteration of the IoT and the smart home are Building36™ and Sonos™. Building36 also aims to automate the house in a similar manner as Nest Labs, with plumbing, gas, and electricity all controllable from a centralized application. Sonos is targeting a different market, with a wifi-enabled speaker that fits in seamlessly as another household appliance. With the help of these companies and their products, today's average homeowner can interact with their house through voice commands and applications and control parts of their house that were once manually controlled.

Security Issues

The smart home remains an exciting advancement in technology; with it comes several important risks as well as larger applications in the future. One of the big issues with IoT today is security. Many internet-enabled devices struggle to be secure, often trading strong security for a lower cost of production. In just the past couple years, three major attacks brought down services such as Netflix™, Spotify™, and Twitter™ through the exploitation of IoT memory limitations (Wallen, 2017). A study examining the potential risks underlying home automation found risks in several different categories– software, hardware, information, communication, and human. Regarding software, problems with inadequate authentication in apps as well as vulnerabilities in larger services such as Microsoft Azure™ were unearthed. With the hardware, physical risks included theft and destruction. A lack of authentication found also allowed for data leakage, causing users' personal information to potentially be revealable. Communication channels faced a similar issue. Many of the risks found fell into the human component, with social engineering being a large issue and lax security measures on the homeowners' part (Jacobsson, Boldt and Carlsson, 2016). IoT also introduces a new form of burglary, with individual's digital identities and personal information now at risk (Casey 2015). With these issues exposed, changes need to be made to the production and design of IoT devices for the smart home to be a safe and viable option for the general public. If these issues are address, an extension of the smart home can grow– the smart city. A smart city is an extension of the smart home– when a city begins to use data collected from sensors to operate more efficiently and safely. This effect can be most pronounced in reducing congestion due to traffic jams, as well as reducing energy consumption city-wide through the throttling of electricity during non-peak hours (Meola, 2016). Many cities can benefit from the introduction of IoT integration, but few can pull it off. Solid technological and social infrastructure are key prerequisites for a smart city (Scuotto 2016). The smart city is currently a work in progress, with places like Amsterdam beginning to explore the possibilities. However, with so much at stake, security must be robust in order to safely provide a path forward.

Conclusion

With so much possible through the adoption of the smart home, IoT remains an exciting, impactful, and booming industry. It is with this excitement that drives us to develop our IoT smart fridge. This project builds on all of these past innovations, from the smart home to the home assistant. Without these predecessors, we would not be able to create our product as easily. The goal for our project is to continue the current growing trend of IoT devices geared towards the average homeowner or renter. We do face the same challenges as the general IoT community, including security and adoption by the general public. A major challenge we have encountered is ensuring that our product is not only economically viable and technically sound, but also has the ease of use to facilitate regular usage. Even with IoT's ever present issues, they are addressable and still allow for an optimistic look into the future of IoT. As time goes on, the smart home will likely continue to grow through adoption by homeowners and improvements from manufactures.

References

1. Casey, E. (2015). Smart home forensics. Digital Investigation, 13, A1-A2.

2. Gabbai, A. (2015). Kevin Ashton Describes "the Internet of Things". Smithsonian. [Accessed 1 Dec. 2017].
3. Jacobsson, A., Boldt, M. and Carlsson, B. (2016). A risk analysis of a smart home automation system. Future Generation Computer Systems, 56, pp.719-733.
4. Meola, A. (2016). How smart cities & IoT will change our communities. [online] Business Insider. [Accessed 1 Dec. 2017].
5. Rothfeld, L. (2015). Home smart home: A history of connected household tech. Mashable. [Accessed 1 Dec. 2017].
6. Scuotto, V., Ferraris, A., & Bresciani, S. (2016). Internet of Things. Business Process Management Journal, 22(2), 357-367.
7. Wallen, J. (2017). Five nightmarish attacks that show the risks of IoT security | ZDNet. ZDNet.[Accessed 1 Dec. 2017].
8. Williams, O. (2016). Of course there's an internet-connected rice cooker now. The Next Web. [Accessed 14 Dec. 2017].
9. WIRED. (2017). OK, House. Get Smart: Make the Most of Your AI Home Minions. [Accessed 14 Dec. 2017].