Mark Demore II

ECE 485

Dr. York

22 March 2019

Internet of Things Architecture Draft

***Abstract –* The Internet of Things (IoT) is an ever growing network of “smart” devices. From fridges to streetlights, everything is being integrated into the IoT. With a wide range of devices and networks, IoT architectures are similarly diverse, from the level of a single home to an entire city. Similarly, with a vast set of data, security concerns have been influencing architecture as well. Rapid hardware and protocol growth and development has only expedited this integration, and will continue to do so, potentially posing a greater risk if this growth continues unimpeded without proper security measures.**

1. INTRODUCTION

The rapid growth of IoT has been highlighted by an increased interest from major technology firms, such as Amazon and Google. Previously, the focus of IoT was the smart home, leading the charge was Phillips with their smart bulbs and an expensive, cumbersome hub that was the center of their network, controlling all other devices. Now, many different manufacturers are producing smart devices that can be easily incorporated across brands and protocols, with some taking a homebrew approach. On the other hand, many are realizing the industrial capabilities that IoT provides, as well as municipalities taking initiative to create smart cities. Power grids are now integrated with the IoT, many manufacturers have implemented IoT on their production lines, and cities are now using IoT to communicate between organizations in real time and provide better services to their citizens.

This work discusses the various architectures used for IoT, their applications, and effectiveness, with a focus on architectures for smart cities. It also addresses areas of concern, particularly for security, and a look at the future of IoT integration.

1. BACKGROUND

IoT architecture, for the purposes of this paper, will be divided into the following parts: Hardware, Protocols, Security, and Network Design. Hardware describes the many devices in a smart network, from a phone to a controller or hub. Protocols describe the way the devices communicate with one another; wi-fi, Bluetooth, or Zigbee. Security will primarily be used to distinguish whether or not smart devices have their own internal security or if they rely on network security alone. Finally, network design will be used to describe how the network is configured, which will rely primarily on the application of the smart network; home, warehouse, city, etc.

Internet of Things encompasses practically any device that can connect to the internet. Each device serves as a sensor that passes data, acting as feedback in a closed control loop, which allows the controller to make decisions. In the case of the smart home, a camera in a fridge might notice that there is no milk, and tell the controller which will send an SMS to the owner. Another sensor might notice that the occupant is not home during certain hours and inform the controller which will then adjust the thermostat to conserve energy during those hours. A small, $20 Particle Photon board attached to a mailbox might activate when opened and tell the controller to send an SMS letting the owner know that the mail has arrived. Expand these basic ideas to a factory or a city, and the benefits grow exponentially, allowing for advanced automation and increased efficiency.

IoT architecture can also be described in 3 layers; perception, network, and application [4]. The perception layer is the devices that are acting as sensors. The application layer is where the output is applied, such as a smart home. The network layer is everything that connects the other two layers together, the wireless protocols and the controllers that process the data.

1. SMART CITIES

With the amount of data that can be captured by IoT devices, there is a vast number of benefits for integrating this technology into a city’s infrastructure. Power grids can use IoT to more efficiently distribute power and save resources when they aren’t needed. Public transit can use big data to coordinate and optimize routes. With IoT technology, manufacturers can optimize production lines, and buildings can reduce energy consumption. The most largely beneficial applications of IoT in a smart city are in education and health. Not only can buildings and utilities adapt based on the feedback from IoT sensors, but data on students and patients can be easily tracked and used to provide better services. Given the scale of developing a smart city, there are many challenges that need to be addressed.

In order to provide for this large infrastructure, the focus of a smart city would be closely related with big data. Processing all of this user data in order to make decisions, while extremely intensive, has become more manageable with the progress that has been made with handling and analyzing big data. Given the range and variety of devices, the protocol for most smart cities would be either LTE or 5G based. The networking scheme for a smart city would mimic a mesh network, integrating controllers and the variety of devices. Despite all the benefits this provides, the metadata that it creates can be exploited. The easiest security method to implement in this case is air gaps, separating components and keeping them as part of their own private network and not one that can be reached from the outside.

When attempting to make cities “smarter”, the biggest challenge they face is infrastructure. Particularly, cities struggle to combine data from multiple sources and with having enough computing power to process the data and provide a timely output [8]. One way of addressing this is through a multi-core architecture with various levels to aid with automation [8]. However, Internet of Things networks are susceptible to the same attacks and exploitations as any other network. Particularly, Distributed Denial of Service (DDoS) attacks could disrupt automation and prevent the flow of vital information in a smart city, which could be catastrophic without a failsafe [6].

A number of other attacks could pose a great risk to smart cities. Spoofing would allow an attacker to provide false data as input to the system which could be used to manipulate the system. More commonly, stolen data would lead to a violation of privacy for citizens of a smart city, leaking anything from their current location to their medical records.

With new developments in 5G technology, smart cities will become even easier to connect. Most modern control systems are already built with the necessary features to join an IoT network, including power grid relays. 5G will allow communication among the cityscape with speed and ease, in order to allow for more remote monitoring and real time response.

1. HOMEBREW TECHNOLOGY

While IoT technology can be expanded to a number of industries and on a large scale, most recent developments have been a result of homebrew technology. While IoT initially started with a few brands releasing products that could only communicate with each other, since it has grown a number of products have been released that allow for more open source adaptations. This has allowed for incorporation across devices and protocols. It has also created the opportunity for increased security.

The Particle Photon board highlights the flexibility of homebrew technology. The Photon is a small microcontroller board, complete with wi-fi, Bluetooth, or 4G headers. It allows a number of sensors to be placed remotely and communicate with a central controller, and for under $20, it opens up plenty of new windows for the Internet of Things.

The increased ease of access to microprocessors, microcontrollers, and other single board computers, has allowed homebrew technology to fill seemingly any space in an almost Rube Goldberg-esque manner. This has allowed for development in home automation as well, and has been furthered by a new interest in solar power and power walls.

1. LOOKING FORWARD

With the rapid growth of the Internet of Things, summarized by the current 4 connected devices per person globally, there are many new applications of this increase in information. A number of researchers are currently interested in the potential for a decentralized internet, which could greatly improve latency. But, before any new growth, privacy and security concerns need to be addressed. Another potential use of IoT is automation, in an extreme way. With IoT, smart cities could have autonomous transportation that is constantly becoming more efficient, particularly if coupled with machine learning technology. Factories could entirely automate their production and shipment of their products. The possibilities are nearly as numerous as the many types of devices that now make up the Internet of Things.

As other tech improves, it will also be adapted for purposes in line with IoT as well. New data will find a way to be used in order to make processes more efficient, automate them entirely, or streamline the sharing of data across organizations. Amazon’s new store with no checkout is a prime example of how IoT can be used. By tracking customers and items, totals can automatically be calculated and charged to the customer’s account. These basic concepts can be further applied to a number of industries to continue automation and ease data sharing. Whether it’s a factory tracking their products and shipments or a hospital tracking patient data, the implications are endless.

1. CONCLUSION

In summary, the internet of things encompasses an enormous amount of devices that are now connected to the internet. Given that each of these devices serves as a sensor, there is an obscene amount of metadata that can be harnessed to increase energy efficiency and the effectiveness of services. Despite privacy and security concerns, mostly based on the pervasiveness of these technologies coupled with their usual lack of security measures, they provide great value to their users and more embedded devices are connected to the internet every day.

Smart cities are at the cutting edge of IoT architectures, incorporating a multitude of devices and protocols, with complex controllers in order to process big data. They also show just how much IoT data can do in terms of optimization, automation, and efficiency. The main issue facing smart cities will be the legal battle with regards to privacy, given the exploitability of metadata, as well as poor infrastructure and networks. Beyond this, homebrew technology is bringing fresh, open source approaches to IoT and new applications. As it continues to grow, devices will provide even more information that will prove even more useful. However, if the growth of the technology is not paced by proper security measures and infrastructure, it may pose more of a threat than it would provide a helping hand. Nonetheless, IoT is the epitome of the Age of Information.

1. REFERENCES

[1] Sahil Sholla, Roohie Naaz, Mohammad Ahsan Chishti. *Semantic Smart City: Context Aware Application Architecture.*

[2] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, Shahid Khan. *Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges.*

[3] Steven M. Beyer, Barry E. Mullins, Scott R. Graham, and Jason M. Bindewald. *Pattern-of-Life Modeling in Smart Homes.*

[4]Siham Al Hinai, Ajay Vikram Singh. *Internet of Things: Architecture, Security Challenges and Solutions.*

[5] Jamie Payton, Xiaojiang Du, Xubin He, Jie Wu. *Envisioning an Information Assurance and Performance Infrastructure for the Internet of Things.*

[6] Ahmet Arı, Sema F. Oktu, Thiemo Voigt. *Security of Internet of Things for a Reliable Internet of Services.*

[7] Miao Wu, Ting-lie Lu, Fei-Yang Ling, ling Sun, Hui-Ying Du. *Research on the Architecture of Internet of Things.*

[8] Basil Nikolopoulos, George Dimitrakopoulos, George Bravos, Alexandros Dimopoulos, Mara Nikolaidou, Dimosthenis Anagnostopoulos. *Embedded Intelligence in Smart Cities through Multi-Core Smart Building Architectures: Research Achievements and Challenges.*