Smart Cities: The Secure Integration of Internet of Things Devices Into City Infrastructure

(Technical Paper)

Internet of Things Devices: Policies and Practices That Impact the Privacy of Consumers

(STS Paper)

A Thesis Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree

Bachelor of Science, School of Engineering

Ranjodh Singh Sandhu

Fall, 2020

Technical Project Team Members

Karanvir Singh Jassal

Justin Hoon Kim

John Daniel Light

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

Signature  Date 11/03/2020

Ranjodh Singh Sandhu

Approved  Date 11/03/2020

Aaron S. Bloomfield, Department of Computer Science

Approved _____ Date _____

Kathryn A. Neeley, Associate Professor of STS, Department of Engineering and Society

Introduction

Innovation has often stemmed from a desire to complete tasks more efficiently or conveniently. The ability to automate the process of data collection and application has revolutionized the way information is communicated and has the potential to impact society in a magnitude that has been unmatched since the creation of the Internet itself. The Internet of Things (IoT) has been rapidly growing in recent years. In 2018, there were around 7 billion IoT devices with an estimated growth to 20-50 billion devices by 2020 (Allhoff & Henschke, 2018, n.p.). While the Google Home and Amazon Echo are common examples of IoT devices, but IoT goes much deeper. Allhoff & Henschke (2018) stated that it consists of "a complex network of interactive and technical components clustered around three key elements: sensors, informational processors, and actuators" (n.p.). There is no widely accepted definition for the term *smart city*, but the purpose of them is to increase the efficiency and quality of the services offered by public administration to the citizens. The IoT plays a significant role in this goal as it is a "communication infrastructure that provides unified, simple, and economical access to a plethora of public services" (Zanella, Bui, Castellani, Vangelista, & Zorzi, 2014, p. 22). A basic example of this concept is a network of connected street lamps that would enable a city to monitor the status of all of the lights from a central location. This way, if a bulb burns out or there is a malfunction, the city could be notified instantly and can address the issue. In this instance, the street lamps would be IoT devices and this technology, combined with many other possible sensors communicating on the same network, would form the smart city. In the simplest description, a smart city is the application of the Internet of Things in a city-wide scale.

With the increased usage of IoT devices and their potential implementation into smart cities, it is important to understand the capabilities of these devices. Allhoff and Henschke

(2018) found that there have been “a series of cases already where smart televisions and other smart devices have been sent data picked up by cameras and microphones from people's homes back to the producer's servers for analysis, without clear or obvious consent from the users” (n.p.). Currently, cities are not reaching their full potential of efficiency and have room to make life much easier for citizens. However, the privacy concerns that come with the usage of the IoT in a scale this large may act as an obstacle for the implementation.

In an attempt to address the inefficiency that currently exists in cities, the technical project outlined in this prospectus seeks to deliver a design for the widespread implementation of secure smart cities. The STS research will focus on the current usage of the IoT and how it has impacted the privacy of users. With the growing popularity of consumer IoT devices, it is important to understand what these gadgets track and how the data is then used.

Technical Topic: Designing a Secure Smart City

The continuous advancements in the Internet of Things has led to the concept of smart cities and subsequent efforts to begin implementation of smart cities. For example, there is a proof-of-concept smart city that has been integrated into Padova, Italy. One of the main goals of the Padova Smart City is to “promote the early adoption of open data and [information and computing technology] solutions in the public administration” (Zanella, Bui, Castellani, Vangelista, & Zorzi, 2014, p. 28). The biggest application has been their system for collecting environmental data while also tracking the public street lighting. Installing various wireless nodes (each equipped with a sensor) onto the light poles and connecting them through the Internet has made this application possible. As described by Zanella, Bui, Castellani, Vangelista, and Zorzi (2014), this system has made it possible to “collect interesting environmental

parameters, such as CO level, air temperature and humidity, vibrations, noise, and so on, while providing a simple but accurate mechanism to check the correct operation of the public lighting system by measuring the light" (p. 28-29). While this example is one potential use case of the IoT in a smart city, it involves many devices and layers of linkage. Figure 1 below illustrates the various layers of networking and communication required for the Padova Smart City.

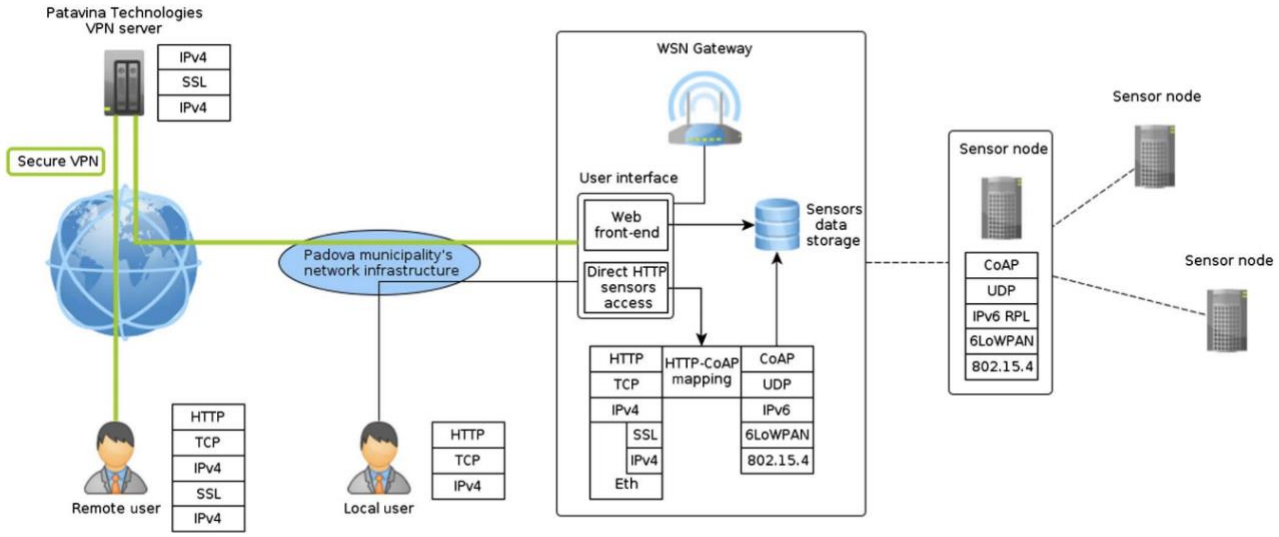

Figure 1: A high-level, conceptual overview of the Padova Smart City system architecture showing the various network levels used to enable the IoT devices to communicate in a secure manner (Zanella, Bui, Castellani, Vangelista, and Zorzi, 2014, p. 29)

It is apparent that there are many different components and layers to the architecture of the Padova Smart City. This, however, is only one example of a smart city and the system architecture it has in place. Smart cities and cryptocurrency raise many of the same security issues. Blockchain technology could be implemented to the IoT platform to "preserve the five basic cryptographic primitives, such as confidentiality, authenticity, integrity, availability and non-repudiation" (Paul et al., 2018, p. 1). This concept covers the same security needs of a smart city. A blockchain architecture can distribute privacy and trust as well as address access control concerns. A design proposed by Paul and his colleagues (2018), consists of three parts: smart

blocks, canopy networks, and cloud storage (p. 2). The smart blocks would be partitions of the city that each own the various sensors used to collect data. The smart block is maintained by a block admin who has legal access to the sensors and output data. The canopy network is the peer-to-peer network that accommodates administrative bodies and police stations. The cloud storage is used to store and share any of the data collected by the sensors (Paul et al., 2018, p. 2). Figure 2 provides a visualization of the concept.

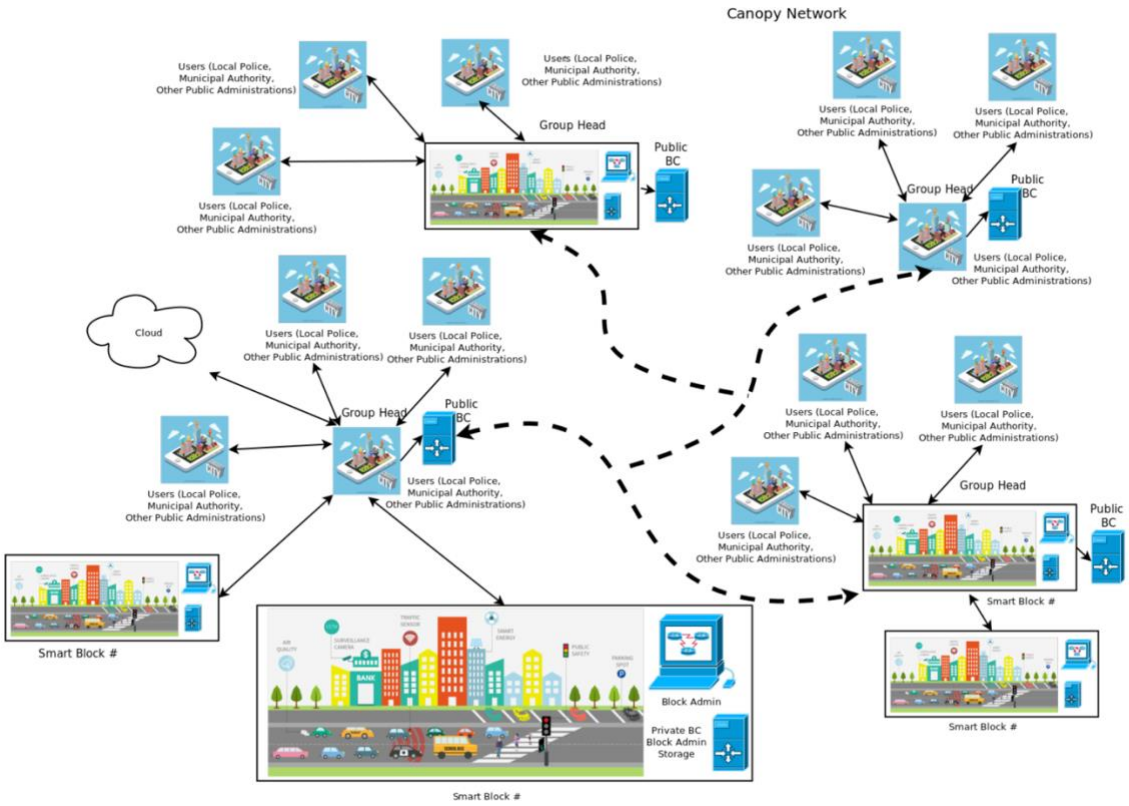

Figure 2: A high-level, conceptual overview of the blockchain system architecture (Paul et al., 2018, p. 4)

Regardless of the architecture implemented in a smart city, there is another component that will ultimately determine the success of the security. A smart city consists of not only these advanced devices but also "humans – municipal workers, citizens, visitors and business people

piggybacking onto municipal wifi systems – who are often weak links in the cybersecurity chain because of poor security hygiene" (Pasha, 2020, n.p.). One main obstacle of creating a secure smart city will be educating policymakers and actors involved with the use of the devices. As shown in Figure 3, there are both IT and organizational challenges that come with the implementation of smart cities. It is imperative that those with access to the network and data of the smart city follow safe practices.

Dimension	Challenges
IT skills	• IT training programs • Lack employees with integration skills and culture
Organizational	• Lack of cross-sectoral cooperation • Lack of inter-departmental coordination • Unclear vision of IT management • Politics • Culture issues

Figure 3: Challenges of using technologies in smart cities (Chourabi et al., 2012, p. 2292)

Failing to understand the security needs of a smart city and the technology behind it will lead to a premature implementation. Smart cities will constantly be under cyber-attacks and being ill-prepared would result in breaches. The distrust in the government after unsuccessfully defending against a smart city cyber-attack would lead to the downfall of the smart city concept itself. Smart cities have the potential to make economic and environmental impact and failing to implement smart cities as a whole will result in a missed opportunity. Environmentally, applications of IoT "such as building-automation systems, dynamic electricity pricing, and some mobility applications could combine to cut emissions by 10 to 15 percent" (Woetzel et al., 2020, n.p.). In addition, tracking water consumption and air quality could help signal the urgency of the situation and push for change. Educating citizens with data and statistics representing their region of residence may impact them more than hearing about other places.

Economically, the data that the devices provide can help make better decisions. Ellsmoor (2019) used the example of how "the United Kingdom has plans to integrate smart technology in future development and use big data to make better decisions to upgrade the country's infrastructure. Better decisions could be a boom to the economy" (n.p.). In addition, the task of transitioning to a smart city will also open up more jobs and create long-lasting jobs to maintain the technology. According to Chourabi and his colleagues (2012), the implementation of smart cities has the potential to produce the economic outcomes of "business creation, job creation, workforce development, and improvement in the productivity" (p. 2293). An analysis of various proof-of-concept smart cities that have been established can provide insight into both the successes and challenges involved with the transition.

STS Topic: Analysis of Current IoT Usage and its Impact on Privacy

A major component of smart cities will be the devices that are used to collect the data. In a smart city, these devices would be everywhere and always recording data. It is important to understand the capabilities of these devices especially since the long, unclear privacy policies make it difficult for the average consumer to understand what data is being gathered and how it is being used. Allhoff & Henschke (2018) illustrated a strong example of the privacy issues through a "widely publicized case [where] Target mined a client's purchasing habits, predicted that she was pregnant, and [sent] a mailer promoting baby items to her home. As it turns out, she was still in high school and, while she was in fact pregnant, her family did not know; they literally found out because of the mailer" (n.p.). There is a high probability that the girl was not informed that her purchasing habits were being tracked and it was a clear misuse of her

information. This situation was from a website that she was choosing to use but imagine what devices that are around all the time regardless of one's choice have the potential to track.

Failure to address the privacy concerns that come with the usage of IoT devices will result in significant push back from the public. One of the major factors for citizens "comes from concern that their data are used for other purposes than they were originally collected for" (Zoonen, 2016, n.p.). Data collected on that level can be very valuable for some companies. Zoonen (2016) uses two examples to highlight how this has been done in the past. The first was "when, in The Netherlands in 2014, ING bank announced that it would share its client data with commercial parties, immediate public anger arose, people changed banks and in the end ING withdrew their plans and was forced to apologize" (Zoonen, 2016, n.p.). The second example was when the UK National Health Service faced heat after "it appeared that the medical records kept by general practitioners would not only be shared with other health and care institutions, but also with commercial third parties, most notably health insurance companies" (Zoonen, 2016, n.p.). Similarly, this raises the concern of who is dealing with the data.

It is important to address whether these privacy concerns are warranted and if they will outweigh the benefits of a more efficient lifestyle. For example, the application of technology for public safety and stopping crime can greatly benefit the community. But, on the other hand, the systems that would need to be put in place may raise concerns about people's privacy. Woetzel and his colleagues (2020) highlighted this by stating "applications such as gunshot detection, smart surveillance, and home security systems can accelerate law-enforcement response. But data-driven policing has to be deployed in a way that protects civil liberties and avoids criminalizing specific neighborhoods or demographic groups" (n.p.). GPS monitoring raises a similar concern. While it has many applications to benefit citizens such as speeding up help from

first responders, the data has the potential to hurt citizens as well. The government can store GPS data and mine them for years following without the knowledge of those who are being tracked. As with smart city data as a whole, GPS data "could have a negative impact on freedoms of speech and association with others as well as provide the government with immense private information subject to misuse" (Elmaghraby & Losavio, 2014, n.p.).

Limiting the scope of IoT devices may help establish a middle ground where efficiency has still increased but privacy is not compromised. This will largely depend on the government and how it decides to proceed. In situations like this, transparency is crucial in order to gain the trust of the citizens. Allhoff & Henschke (2018) assert that "there needs to be a standard that establishes informed consent for the acquisition, retention, and sharing of personal data. For example, the European Union has recently implemented a definition of consent as: 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'" (n.p.).

In order to achieve this goal, it is important to understand the various rights and liberties of citizens as well as how they are applied in the context of modern-day technology. One of the biggest challenges of using technology with the government is how fast the technology grows beyond the comprehension of government officials. In order for smart cities to be successful, it is imperative that government officials are well-educated on the technology and concepts. Education on technology will not only ensure a more secure practice but also enable a smoother transition. Hayduk (2016) highlighted that "falling behind puts us at risk of two distinct threats. On one hand, advancement and adoption may be stifled by concerns about murky policy or a

lack of accepted technological standards. On the other, innovation without thoughtful oversight raises the specter of security, privacy and ethical breaches" (n.p.).

The example of how the IoT can impact the citizens around it is clearly related to sociotechnical systems. The use of STS concepts such as Actor-Network Theory and problem definition will allow for a clearer understanding of what needs to be adjusted in IoT technology to better suit the concerns of the people. Prior research on the misuse of information and data as well as research on better use cases can be built upon to establish a middle ground where policy is enforced to uphold civil rights and liberties.

Conclusion

Continuing advancements in the Internet of Things that maintain ethical practices and privacy for the users will enable the development of smart cities to transform the lives of citizens. The technical portion of my thesis will come together during the spring with a design of a smart city that minimizes the intrusion of privacy. The STS research will yield a better understanding on how the IoT impacts the privacy of users and whether it is justified.

While the proposed design will be primarily conceptual, the government and contractors may implement the idea itself into an actual smart city. This integration will allow for more successful smart cities that are supported by the citizens, which would kickstart the movement. The government and citizens will be able to enjoy the benefits of the smart cities without having conflict over privacy. By working to eliminate obstacles that are slowing down the growth of smart cities, cities can begin to increase the quality of life for their citizens as well as stimulate the economy while reducing environmental impacts.

References

Allhoff, F., & Henschke, A. (2018). The Internet of Things: Foundational ethical issues. *Internet of Things, 1-2*, 55-66. doi:10.1016/j.iot.2018.08.005

Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., . . . Scholl, H. J. (2012). Understanding smart cities: An integrative framework. *2012 45th Hawaii International Conference on System Sciences*. doi:10.1109/hicss.2012.615

Ellsmoor, J. (2019, May 19). Smart cities: The future of urban development. Retrieved October 08, 2020, from https://www.forbes.com/sites/jamesellsmoor/2019/05/19/smart-cities-the-future-of-urban-development/#6f4c24cb2f90

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research, 5*(4), 491-497. doi:10.1016/j.jare.2014.02.006

Hayduk, J. (2016, June 29). The other 2016 cycle: When technology outpaces policy. Retrieved October 21, 2020, from https://www.vox.com/2016/6/29/11978162/regulation-business-2016-cycle-technology-outpaces-policy

Pasha, Haider. (2020, March 26). This is how we secure smart cities - what leaders must consider. Retrieved October 20, 2020, from https://www.weforum.org/agenda/2020/03/this-is-how-we-secure-smart-cities/

Paul, R., Baidya, P., Sau, S., Maity, K., Maity, S., & Mandal, S. B. (2018). IoT based secure smart city architecture using blockchain. *2018 2nd International Conference on Data Science and Business Analytics (ICDSBA)*. doi:10.1109/icdsba.2018.00045

Woetzel, J., Remes, J., Boland, B., Lv, K., Sinha, S., Strube, G., . . . Tann, V. (2020, September 14). Smart cities: Digital solutions for a more livable future. Retrieved October 08, 2020, from https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/smart-cities-digital-solutions-for-a-more-livable-future

Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of Things for smart cities. *IEEE Internet of Things Journal, 1*(1), 22-32. doi:10.1109/jiot.2014.2306328

Zoonen, L. V. (2016). Privacy concerns in smart cities. *Government Information Quarterly, 33*(3), 472-480. doi:10.1016/j.giq.2016.06.004