BUILIDNG SAFER SMART CITIES: GUIDELINES TO ENCHANCE FUTURE SECURITY INFRASTRUCTURE FOR INTERNET OF THINGS DEVICES

A Research Paper submitted to the Department of Engineering and Society
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Engineering

By

Cameron Davis

August 5, 2022

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.

ADVISORS
Catherine D. Baritaud, and Bryn Seabrook, Department of Engineering and Society

EXPLORING THE USE OF INTERNET OF THINGS DEVICES IN THE DEVELOPMENT OF SMART CITIES

The Internet of Things (IOT) refers to networks of individual “smart devices” that are used to connect and exchange data. In a modern social context, IOT devices have become strongly associated with popular consumer products, such as the Apple Watch or Amazon Alexa, that hold significant amounts of private user data including health and financial information. At a global scale, urban planning has shifted towards designing “smart cities” that focus on sustainability. By using ubiquitous IOT sensors to collect data points, designers aim to reduce electricity use and carbon emissions, protect wildlife by tracking animal movement patterns and mitigate other environmental issues. Since the use cases for IOT technology vary widely by industry, the lack of standardization in security protocols leave devices vulnerable against security breaches and make it difficult to ensure a high level of protection for all devices (Das, 2018).

The STS thesis explores the privacy, security and ethical issues associated with IOT solutions in “smart cities” using the theory of Social Construction of Technology (SCOT). Society’s interaction with IOT technology has created the need for appropriate security measures yet there are no unified technical or government standards for manufacturers or developers. In order to fully utilize SCOT, “the five components — relevant social groups, interpretation, closure, technological frame, and the wider social context” (Klein, 2002, p.36) are used to properly contextualize and explain various terms and roles related to IOT security. The combined analysis of each component helps to define both the current problems and future solutions from various perspectives.

The technical thesis tracks the development of a mobile application with a graphical user interface (GUI) that provides a user with live data within a parking lot. The project advised by Prof. Harry C. Powell and completed with classmates Gunther Abbot, Sean Reihani and Nawar Wali, focuses on understanding the difficulty of protecting user data and integrating multiple technologies. While similar technologies exist, the project provides the user with access to internal location data in order to view available parking spots before they arrive to the garage providing a new functionality over previously deployed technology.

The combination of technical and STS thesis provides a detailed path for understanding the complete IOT pipeline from the start to finish while considering its consequences in society. Privacy and security flaws mainly stem from shortcomings in technical guidelines or government policies while ethical issues arise in the misuse of user data from consumers of IoT technologies. Understanding the complexity in each of these issues can help develop more reliable security protocols that protect both current and future users. While this work does not aim to directly solve these problems by creating a new set of international technical protocols, a framework will be developed that highlights what considerations should be made during such a process.

EXPLORING THE EVOLUTION OF IOT DEVICES

A BRIEF HISTORY OF IOT

The first IOT device was an innocent technology created in 1982 out of curiosity and convenience. Its purpose was to notify users whether the available Coca-Colas were cold or not via an ARRPANET-connected vending machine developed at Carnegie Mellon University (Vardomatski, 2022). Since ARPANET was only connected to a few elite universities, the use of the technology started to blossom when the world wide web was made public in 1993 and eventually the term “internet of things” was coined in 1999 by technology pioneer Kevin Ashton

(Vardomatski, 2021). It took the next 20 years for IOT to technology to gain global traction and in 2008 the first International Conference on the Internet of Things was held in Zurich, Switzerland. Researchers from all over the globe gathered to discuss papers in the field finally breaking down the previously decentralized nature of IOT development. This would eventually lead to The Global Standards Initiative on the Internet of Things (IOT-GSI) being developed in 2015 to "promotes a unified approach for development of technical standards enabling the Internet of Things on a global scale" (ITU, 2021, para. 2) however it took less than one year before they switched operations to the SG20 committee. As global security support only began in the last 7 years, it's clear that 40 years of rapid innovation has skyrocketed the availability of IOT devices past the current global security standards.

FACTORS AFFECTING IOT ADOPTION

The COVID-19 pandemic created a global semiconductor shortage that slowed the development of many technologies yet the number of global IoT connections still "grew by 8% in 2021 to 12.2 billion active endpoints" (Hasan, 2021, para.1). Ericsson, an international telecommunication company, forecasts that "around 18 billion devices will be related to IoT in 2022" showing that this explosive growth shows few signs of stopping. While raw numbers illustrate that there is a currently a strong desire for the technology, most companies were hesitant to start IOT adoption as they were unsure what value it would bring. Figure 1 on page 5 shows the Technology Acceptance Model, commonly used in business schools to teach students how to understand human behavior when it comes to accepting a new technology.

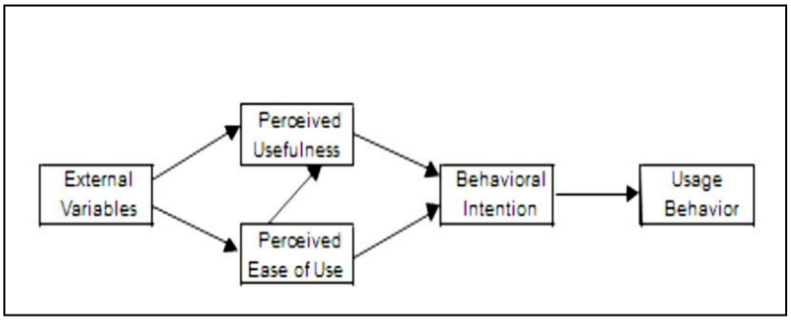


Figure 1: Technology Acceptance Model (TAM). This graph details a rudimentary model that models consumer behavior and guides companies' decisions for adopting a new technology. (Venkatesh & Davis, 1996)

The two main variables in this model are "Perceived Usefulness" and "Perceived Ease of Use". The model was used to conclude that that most consumer technologies made the users perceive their lives as "better", showing why those numbers are quickly rising. Figure 2 below takes a more liberal approach by defining several factors using the diffusion of innovation (DOI) and technology-organization-environment frameworks (TOE) to identify what drives IOT adoption at the corporate level. Comparing the two models quickly illustrates how complex IOT becomes when accounting for other factors than end usefulness.

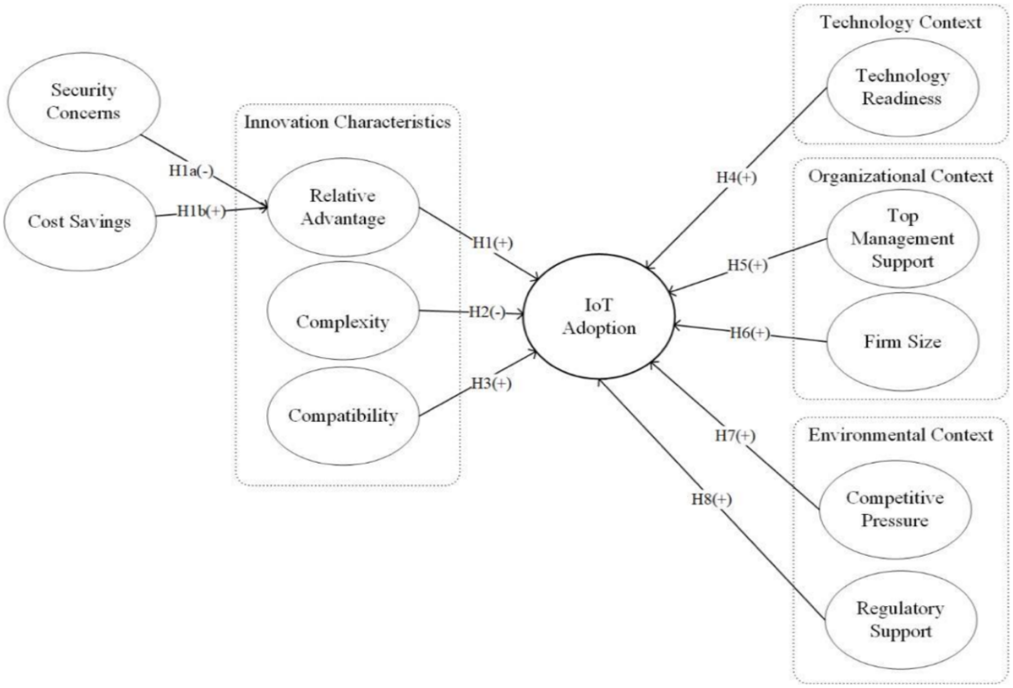


Figure 2: Influence Graph. The model is derived from two technological frameworks and describes eleven unique factors that businesses can use to determine whether to adopt IoT devices into their line of products. (Oliveira, Thomas, & Espadanal, 2014).

From left to right, the model defines these factors from which businesses make adoption decisions: outside factors, innovation characteristics, and technical and social contexts. Most of the factors focus on what adoption looks like relative to their competitors, consumer support and easiness of adoption. This model allows "security concerns" to fall into the outside factors in this model but it remains a central component to ethical engineering practices whose duty is to protect society. From January to June of 2021, there were approximately 1.51 billion breaches of IoT devices (Kaspersky, 2021) meaning that roughly 12.4% of connected IOT devices were successfully attacked. Security must be constantly updated during the IoT lifecycle, which creates a unique challenge for both consumers and manufacturers. As a relatively new field, IoT devices lack a standardization of security protocols which make it difficult to ensure a high level of protection for all devices (Das, 2018).

URBANIZATION AND THE IMPORTANCE OF SMART CITIES

As the global population rapidly expands, data shows that people are moving from rural areas to urban areas at an increasing rate, a phenomenon known as urbanization. In a report conducted by The United Nations, researchers project that by 2050 approximately 68% of the world's population will live in an urban environment (United Nations, 2018). The increase in population has been directly linked with an increase in pollution. IoT is on track to become a central pillar of urban development, as a 2015 projection expected cities to spend $41 trillion on IoT across the following two decades (Adler, 2020, p.2). If IoT devices are the proposed solution, there is a need for society to understand the comprises it might have to make to adopt these advancements. The major influences from IOT technology that affects users revolve around privacy rights and regulatory standards. The lack of laws that properly govern this space “stem from integrating devices into our environments without us consciously using them” and that integration is continuing at an exponential rate. (Banafa, 2017, para. 4). The lack of awareness from users and lack of regulation can also lead to misuse of this data, leaving users vulnerable to companies willing to sell their data to third parties. This concern requires added regulation so users can avoid an increased risk compared to the benefit of using the system (Vasilomanolakis, 2015).

RELEVANT SOCIAL GROUPS

General Consumers

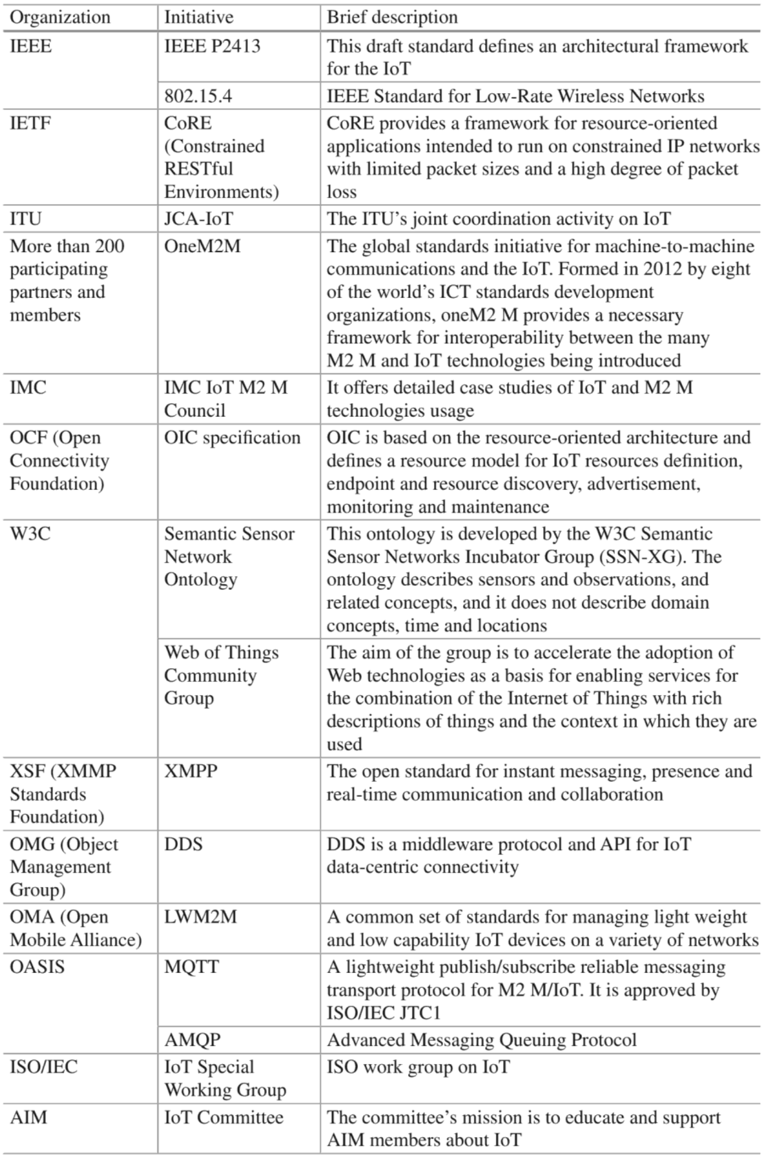
Current urbanization methods have taken a toll on the environment: higher air pollution rates due to increased smog from vehicles, habitat fragmentation as animals are forced out of their homes and lower water quality due to rain absorbing the extra carbon monoxide into the water supply. These malignant effects directly impact the health of the individuals in those areas like Brazil, where strong links have been found between exposure to traffic-related air pollution and developing asthma (Ponte, Eduardo Vieira, 2018). Governments implementing smart city IOT solutions usually support ideas that have the support of its people. In this case, the environmental effects are usually seen in one’s long-term health. Since consumer IOT revolves around improvement in one’s personal life, users are not usually aware of how the technology can affect them at an infrastructural level. Common IoT devices like the Apple Watch have created a comfort level between society and this new technology. This lack of awareness becomes evident when considering users lack of “proper digital hygiene”, defined as changing passwords on a regular basis, using different passwords or logging out of their accounts when finished using a public computer (Vasilomanolakis, 2015). An implicit trust is placed in the designers of these tools; trust that they will make working and secure devices. While they often work, it usually requires some effort on the end users' part to keep it secure. Such as health insurance companies or hospitals who could upcharge customers if they are able to associate with a specific user with unusual health factors.

Companies, Engineers and Shareholders

Ultimately, the main of a company is to maximize profit for their shareholders. This tends to contradict any focus on security in the IOT space due to a lack of government regulation. While the number of connected devices has increased, "only a minority of firms have Internet of Things [security] initiatives" and that "and only a lesser percent of them have effectively incorporated Internet of Things frameworks" showing that protecting these devices is an afterthought to profit. (Ives, Palese, & Rodriguez, 2016, p.1). Companies can prioritize getting a working product on shelves rather than focus on any penalties or fines for lacking security features. From an engineer's perspective, there is difficult considerations where manufacturers may have to provide super-user accounts or backdoor access. It's difficult to ask engineers to provide a way that defeats all the security they built in the first place as that "backdoor" will become the new target for attackers rather than protected individual devices.

Governance and Lawmakers

The laws surrounding the internet have had trouble maintaining innovation at the same rate as the technologies they govern. The United Kingdom's Product Security and Telecommunications Infrastructure bill (PST) was their most recent legislation to address "legislation that requires IoT manufacturers, importers, and distributors to meet certain cybersecurity standards." (Page, 2021, para. 2). One regulation in the bill called for providing each device with private password, but designers oppose this case as it would remove any backup protocols for if a user is locked out of an account. This seems like an ideal approach unless you are the engineer who has to design a system because “if each device has a private password, then who is responsible for managing this?” (Page, 2021, para. 8). A brief description of several standards and committees that oversee IoT technologies can be seen on the right-hand side of Figure 3 below. Balancing these different legislations is a huge challenge as the table shows that many of these legislations aim to solve the same issue.



Organization	Initiative	Brief description
IEEE	IEEE P2413	This draft standard defines an architectural framework for the IoT
	802.15.4	IEEE Standard for Low-Rate Wireless Networks
IETF	CoRE (Constrained RESTful Environments)	CoRE provides a framework for resource-oriented applications intended to run on constrained IP networks with limited packet sizes and a high degree of packet loss
ITU	JCA-IoT	The ITU’s joint coordination activity on IoT
More than 200 participating partners and members	OneM2M	The global standards initiative for machine-to-machine communications and the IoT. Formed in 2012 by eight of the world’s ICT standards development organizations, oneM2 M provides a necessary framework for interoperability between the many M2 M and IoT technologies being introduced
IMC	IMC IoT M2 M Council	It offers detailed case studies of IoT and M2 M technologies usage
OCF (Open Connectivity Foundation)	OIC specification	OIC is based on the resource-oriented architecture and defines a resource model for IoT resources definition, endpoint and resource discovery, advertisement, monitoring and maintenance
W3C	Semantic Sensor Network Ontology	This ontology is developed by the W3C Semantic Sensor Networks Incubator Group (SSN-XG). The ontology describes sensors and observations, and related concepts, and it does not describe domain concepts, time and locations
	Web of Things Community Group	The aim of the group is to accelerate the adoption of Web technologies as a basis for enabling services for the combination of the Internet of Things with rich descriptions of things and the context in which they are used
XSF (XMMP Standards Foundation)	XMPP	The open standard for instant messaging, presence and real-time communication and collaboration
OMG (Object Management Group)	DDS	DDS is a middleware protocol and API for IoT data-centric connectivity
OMA (Open Mobile Alliance)	LWM2M	A common set of standards for managing light weight and low capability IoT devices on a variety of networks
OASIS	MQTT	A lightweight publish/subscribe reliable messaging transport protocol for M2 M/IoT. It is approved by ISO/IEC JTC1
	AMQP	Advanced Messaging Queuing Protocol
ISO/IEC	IoT Special Working Group	ISO work group on IoT
AIM	IoT Committee	The committee’s mission is to educate and support AIM members about IoT

Figure 3: International IOT Standards. This figure shows a table listing 14 different committees and standards from various countries that have different goals in regulating IoT technology (Mahmood, 2018, p.89).

GUIDELINES FOR IOT SECURITY PROTOCOLS WITH PEOPLE IN MIND

The use of IOT technology in smart cities provides a unique opportunity to redefine how people interact with one another and with infrastructure around them. To safely proceed in that endeavor, three areas of concern must be addressed in existing IoT protocols: insufficient security in current IoT implementations, insufficient detailed and specific IoT guidelines in current IT security standards, and insufficient IoT laws and regulation at the country and international level (Ahlmeyer & Chircu, 2016). Each of these categories align with one of the relevant social groups identified using SCOT and using the given context, several guidelines will be laid out to create solutions that aim to satisfy a global audience.

The first recommended guideline would require comprehensive technical education to be central for any future IoT framework. Since focusing on IoT security standards remains an afterthought for most companies, this concept can return agency back to users of those products. Explaining technical concepts to the public remains a difficult task, however, everyone deserves to have accessible knowledge to the risks they take on when using IoT technologies. To consider the economic barriers that would prevent users from accessing IoT at a consumer level, governments can supports STEM education programs in underserved communities so that consumers are able to understand their digital privacy rights without having their own smart device.

The second guideline attempts to change a traditional model by incentivizing businesses with tax breaks given that they allow a government sponsored specialist check their security standards. Aided by the DOI-TOE model shown earlier in Figure 2, it seems critical to involve business model frameworks when considering security implementation into IoT devices. This branches off the first guideline because if users are educated about why they should care about security, they can vote with their wallets. Tax breaks give businesses a financial benefit for adhering to the rules while not directly providing them with more funding. This would help businesses focus on their end users' desire, in this case, protecting their own security.

The third guideline looks to address the issues of what frequencies certain devices can use, an important the technical barrier faced by engineers and manufactures. Each country would list a range of radio frequencies according to device usage that would be assigned to manufacturers, similarly to how internet protocol addresses are distributed for websites. One of the challenges faced during the technical project was that many types of connections exist for such a simple device.

REFERENCES

Adler, L. (2020). The urban Internet of Things. *Data-Smart City Solutions*. https://datasmart.ash.harvard.edu/news/article/the-urban-internet-of-things-727.

Ahlmeyer, M., & Chircu, A. M. (2016). Securing the Internet of Things: A review. *Issues in Information Systems*, *17(4)*, 21-28. https://doi.org/10.48009/4_iis_2016_21-28

Banafa, A. (2017, March 14). Three major challenges facing IoT. *IEEE Internet of Things.* https://IoT.ieee.org/newsletter/march-2017/three-major-challenges-facing-IoT.html/.

Cynthia, J., Sultana, H. P., Saroja, M. N., & Senthil, J. (2018). Security protocols for IoT. *Studies in Big Data Ubiquitous Computing and Computing Security of IoT*, 1–28. https://doi.org/10.1007/978-3-030-01566-4_1 - proper doi apa format

Das, A. K., Zeadally, S., & He, D. (2018, June 28). Taxonomy and analysis of security protocols for Internet of Things. *Science Direct.* https://www.sciencedirect.com/science/article/pii/S0167739X18308112.

Kawamoto, Y., Nishiyama, H., Kato, N., Yoshimura, N., & Yamamoto, S. (2015). Internet of things (IOT): Present state and future prospects. *Tohoku University*. https://tohoku.pure.elsevier.com/en/publications/internet-of-things-iot-present-state-and-future-prospects

Klein, H. K., & Kleinman, D. L. (2002). The social construction of technology: Structural considerations. *Science, Technology, & Human Values*, *27*(1), 28-52. https://journals.sagepub.com/doi/10.1177/016224390202700102

Ericsson. (n.d.). 5G and IoT: Ushering in a new era. *Ericcson.* https://www.ericsson.com/en/about-us/company-facts/ericsson-worldwide/india/authored-articles/5g-and-IoT-ushering-in-a-new-era

Hasan, M. (2022). State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally. *IoT Analytics.* https://iot-analytics.com/number-connected-iot-devices/

International Telecommunication Union (ITU). (2015). Internet of things global standards initiative. *International Telecommunication Union*. https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx

Ives, B., Palese, B., & Rodriguez, J.A. (2016). Enhancing Customer Service through the Internet of Things and Digital Data Streams. *MIS Q. Executive, 15*.

Lane, T. (n.d.). *The "Only" Coke Machine on the Internet*. CMU School of Computer Science. https://www.cs.cmu.edu/~coke/history_long.txt

Mahmood, Z. (2018). *Connected environments for the Internet of Things: Challenges and solutions*. Springer. – proper BOOK apa format

Oliveira, T., Thomas, M., & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information & Management*, *51*(5), 497–510. https://doi.org/10.1016/j.im.2014.03.006

Page, C. (2021, December 4). Is the UK Government's new IOT cybersecurity bill fit for purpose? *TechCrunch.* https://techcrunch.com/2021/12/04/uk-internet-of-things-cybersecurity-bill/

Ponte, E. V., Cruz, A. A., Athanazio, R., Carvalho-Pinto, R., Fernandes, F. L., Barreto, M. L., & Stelmach, R. (2016). Urbanization is associated with increased asthma morbidity and mortality in Brazil. *The Clinical Respiratory Journal*, *12*(2), 410–417. https://doi.org/10.1111/crj.12530

United Nations. (n.d.). 68% Of the World Population Projected to Live in Urban Areas by 2050, Says UN | UN DESA. *Department of Economic and Social Affairs*. www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html#

Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2016). On the security and privacy of internet of things architectures and systems.*2015 International Workshop on Secure Internet of Things (SIoT)*. https://doi.org/10.1109/siot.2015.9

Vardomatski, S. (2022). The history of IoT: A comprehensive timeline of major events, infographic. *HQSoftware*. https://hqsoftwarelab.com/blog/the-history-of-IoT-a-comprehensive-timeline-of-major-events-infographic/

Wei, J. (2014). How wearables intersect with the cloud and the Internet of Things: Considerations for the developers of wearables. *IEEE Consumer Electronics Magazine*, *3*(3), 53–56. https://doi.org/10.1109/mce.2014.2317895