Subtleness of IOTs

Debashis Jena

University of Maryland University College

**MEMORANDUM**

TO: [First Name and Last Name]

FROM: Debashis Jena

DATE: October 11, 2019

SUBJECT: Subtleness of IoTs

**Introduction**

Internet of Things (IoT) was a tech innovation in its early days. However, now it has become one of the most applied technologies in household products and also in automobiles. From being a luxury, IoTs have become a necessity for people to some extent. “According to Helsinki, Finland-based F-Secure, a cybersecurity company citing research from Gartner, over the next two years, the number of IoT devices entering households will climb steeply from nine devices per household currently to 500 by 2022, with IoT connectivity being bundled into products whether people want it or not.” (David Roe, 2018, para. 8). The next couple of years are going to witness a tremendous growth of IoTs and more innovation with and within the technology. The technology consumes a massive amount of data, which makes the predictability of the devices so accurate and precise. Being heavily dependent on data, IoTs come with some unavoidable risks and issues. Apart from data security issues, there have been concerns about cloud attacks. As per the “Global Risk Report (2018)” by World Economic Forum The number of IoT devices has gone beyond the human population on the planet, and the IoT devices do not possess enough out-of-the-box-security (Collins, 2018, page 15). That makes them vulnerable to cyber-attacks. “54 percent of consumers possess an average of four IoT devices.” (Chris Albert, 2018). These are the devices that are apart from regular computers, tablets and mobile phones in their homes. With a standard Wi-Fi router, supplying internet data to so many devices at the same time, the connectivity becomes another issue, leading to a malfunction of the device. Additionally, the lack of IoT literacy in the older age group makes the usage of the technology an inconvenience than otherwise.

The modern time is about smart houses and smart appliances. The era of smart cars is very near. Thus, there are going to be numerous innovations around the technologies in future. Major IoT developers like Google, Amazon are working tirelessly to address these major issues like data security, cyber-attacks, connectivity. There are many viable solutions to these major issues that are impacting the current world economy.

**Discussion of IoT Issues**

IoTs solely work based on the internet, which already has seen major online crimes in the last couple of decades. In addition, most IoT servers are hosted in the cloud. For example, Amazon’s Alexa is an IoT device that constantly streams data back and forth to the Amazon Web Service’s (AWS) cloud service. Cloud services share resources; unless the proper security guidelines are followed, there can be major internal flaws and result in the user data being easily compromised. AWS mandates its customers to read their white papers and recommends consulting with their support engineers while setting up any servers for such IoT devices.

IoTs are built based on artificial intelligence concepts. Some researchers believe that AI has not been that intelligent yet to find the cause and effect in an investigation. So, AI may not be able to prevent the cyber-attacks on the cloud or the IoTs. However, “Experts suggest that malware is now becoming better at evading detection via AI.” (Chris Albert, 2018, para. 6). They expect to use Polymorphic Malware technology and take the most advantage of AI and avoid detection through machine written procedures.

The world economy gets highly affected by cyber-attacks. “The annual economic cost of cybercrime is now estimated at worth of $1 trillion, a multiple of 2017’s record-year aggregate cost of approximately $300 billion from natural disasters.” (David Roe, 2018). In addition, being very complicated network connections, cloud service can be a single point failure for hundreds of businesses, healthcare, and critical government entities. The modern cloud service providing companies like Amazon, Google or Microsoft has a feature of a private network which they otherwise call as Virtual Private Cloud (VPC). These private networks isolate the IoT servers from the other company server accounts. With proper guidelines, the cybersecurity experts can setup these servers with the appropriate inbound and outbound access rules. Thus, the cyber-attacks can be avoided to a large extent.

Connectivity is also a big challenge for IoT devices. Currently, the technology relies on the centralized client-server model, to constantly authenticate the user and serve the devices with appropriate content. With a few million devices, the current model is sufficient. However, when the number of devices eventually increases to billions the centralized model will become a big hurdle. It will require a huge amount of spending to support the ecosystem. Therefore, researchers are coming up with various ways to mitigate the issue by decentralizing the model. “Part of it can become possible by moving some of the tasks to the edge, such as using fog computing models where smart devices such as IoT hubs take charge of mission-critical operations and cloud servers take on data gathering and analytical responsibilities.” (Ahmed Banafa, 2017). Another decentralization technique can be by use of peer-to-peer communication. Devices can communicate among themselves to authenticate each other without reaching out to the servers. This can reduce the back and forth traffic between the server and the client by many folds.

Another challenge that IoTs may face is compatibility and longevity. Since IoT technology is growing very fast, there has been heavy competition between businesses. To become the frontrunner in this race, companies add extra hardware and software to expand the features within the devices. For example, at the present time a smart fridge can have a monitor that displays the content inside, and even keeps track of each food items intelligently. Generally, the fridge like appliances lasts for a decade or more. However, the software or hardware for the IoT within the fridge may get outdated earlier because of the compatibility issues. So, these products become a liability than a convenience. Thus, the manufacturer can either continue supporting these devices for a certain period of time or the software and hardware should be upgradeable.

The next and major concern for the consumers is their privacy. Tracking devices are being fit within smartphones, cars and even smart TVs. “[In TVs], voice recognition or vision features are being integrated that can continuously listen to conversations or watch for activity and selectively transmit that data to a cloud service for processing, which sometimes includes a third party. The collection of this information exposes legal and regulatory challenges facing data protection and privacy law.” (Ahmed Bafana, 2017). Therefore, the devices require consent from the consumer before turning on the tracking feature. After the devices collect the data from the user, they must encrypt the data from end to end. Also, the source of the data must be anonymized.

Currently one of the critical concerns for certain IoT developing companies is "the performance". With an average of 4 devices in a house (apart from the smartphones, watches, computers), all connected to the internet may put a lot of load on the router. This ultimately affects each of the devices, which makes them perform slower than they are intended to. This may cause issues like transaction time outs and other malfunctions. To address this, the developers must design the software and the network in such a way that, it consumes the least amount of the bandwidth that is necessary. This issue can easily be addressed by software developers.

# Conclusion

The Internet of Things has the potential to make our lives easier. However, both customers and businesses have shown serious concerns regarding IoT devices and their security. 65 percent of consumers are concerned about a hacker controlling their IoT device, while 60 percent are concerned about data being leaked. (Roe, 2018). Even though device compatibility may not be a major concern for the customers, security and privacy are the most important factor to win the trust in these devices. Lack of confidence in such an innovation can be a blockage for its mainstream adoption. However, the tech giants like Google and Amazon are building more firewall features and security guidelines around the IoT technology.

**References**

Roe, D. (2018). 7 Big Problems with the Internet of Things. *CMSWIRE.* Retrieved from https://www.cmswire.com/cms/internet-of-things/7-big-problems-with-the-internet-of-things-024571.php

Veltsos, C. (2018). Highlights From the World Economic Forum’s ‘Global Risks Report 2018’. *Security Intelligence.* Retrieved from https://securityintelligence.com/highlights-from-the-world-economic-forums-global-risks-report-2018/

Albert, C. (2018). Problems With the Internet of Things You Need to Know! *DZone.* Retrieved from https://dzone.com/articles/problems-with-internet-of-things-you-need-to-know

Banafa, A. (2017, March). Three Major Challenges Facing IoT. *IEEE.* Retrieved from https://iot.ieee.org/newsletter/march-2017/three-major-challenges-facing-iot.html