IOT IN THE FUTURE: HOW IT WILL SHAPE BUSINESS TODAY.

Daniel Mankey, 2395 Orchid, Conway, AR 72034, 501-269-3262, dmankey90@gmail.com

Mark E. McMurtrey, University of Central Arkansas, 201 Donaghey Ave., Conway, AR 72035, (501) 450-5308, markmc@uca.edu

James Downey, University of Central Arkansas, 201 Donaghey Ave., Conway, AR 72035, (501) 450-5327, jdowney@uca.edu

ABSTRACT

Internet of Things (IoT) has grown more popular over recent years. It is being used in business and consumer applications alike. While we see things transition to this technology, many still believe this is only the beginning with more devices to come online in coming years. This paper will discuss some of the risk and rewards of IoT in business. We'll discuss how IoT is being used within certain business applications and delivered to customers, both internal and external. We'll also touch on various privacy issues included DDoS attacks and other risk. By the end of the paper you'll have a clear understanding of how businesses can utilize IoT to improve their business.

INTRODUCTION

"Internet of Things" (IoT) has grown more popular over recent years. It is being used in business and consumer applications alike. While we see things transition to this technology, many still believe this is only the beginning with more devices to come online in coming years. "The cost of connecting is decreasing, more devices are being created with Wi-Fi capabilities and sensors built into them, technology costs are going down, and smartphone penetration is sky-rocketing. These things are creating a "perfect storm" for the IoT" (Morgan, 2014, p. 1).

IoT is the concept of connecting any device with an on and off switch to the internet or each other via the internet. This includes cellphones, wearables, and thermostats but it can be extended much further than that. Now light bulbs, jet engines, washing machines, HVAC vents, home security, and doorbells are connected to the internet. As stated in Morgan (2014), The analyst firm, Gartner, says that by 2020 there will be over 26 billion connected devices... That's a lot of connections (some even estimate this number to be much higher, over 100 billion). There are many ways that consumers and businesses will be impacted.

Business associated with this technology, providing services and software, will boom. Consumers will be able to save time and money in ways they never thought was possible. Tired of waiting for your shower to get warm? Connect it to your alarm so once your alarm goes off, it will send a signal to your shower to turn on at your optimal temperature. What if you're at work and notice supplies are low? Do not worry about re-ordering, the sensors connected to the shelving or items have already re-ordered the low stock and it arrives today. Nearly every industry will find some process or product that will benefit from IoT. Some of these will involve an end product or service

while others will automate internal processes. The applications are truly countless and new ones are added every day.

PRIVACY

Security and privacy are huge concerns of businesses and consumers regarding IoT devices. The possible consequences of successful attacks could affect lives and safety, indirectly or directly, causing death and destruction. This is a very real issue that needs to be studied and understood by IT professionals. "To provide a good experience, IoT devices advertise the services they offer using a service discovery mechanism" (Taly, Shankar & Boneh, 2016, p. 1). This type of mechanism is not the most secure way for devices to communicate. They also follow the zero-configuration networking charter which is missing an important feature, privacy. In order for clients to discover their IoT device, services transmit wide-ranging information about them. It usually includes delicate information such as the device owner's name, the service type, and hostname. This obviously creates a huge threat when the service is on a private device. According to Taly, Shankar and Boneh (2016, p. 2), "A recent study revealed that 59% of all devices advertise their owner's name in the clear, which is considered harmful by more than 90% of the device owners". Most people and professionals are aware of the associated risk with IoT. Some of the existing risk that plague us today are only intensified by the monstrous size of IoT. The difference comes along with the new technology and "how these Things are designed, what they are used for, how they are deployed and managed (or not managed), and how market forces will influence the development." (Lindqvist & Neumann, 2017, p. 26).

Distributed Denial-of-Service attack

There have been many distributed denial-of-service (DDoS) attacks recently, some of which become very complex. A malware called " Mirai" was used to target DNS services provided by Dyn which affected user access to "major services such as Twitter, Amazon, Tumblr, Reddit, Spotify, and Netflix." (Lindqvist & Neumann, 2017, p. 26). Mirai searches for victims whose source code had been freely published giving it easy access to cause major issues. This is not the first time Mirai had been used but this attack was on many more devices than ever before. According to a statement from Dyn, this attack appeared to involve tens of millions of compromised devices, which exemplifies some of the hazard involved with having large numbers of Things connected to the internet without proper protections. Usually, the devices targeted are user friendly and simple but still powerful enough to be a part of the distributed attack. The owners of these devices are frequently not aware their devices are being used to attack other systems.

Vulnerabilities

Apparently, many of the devices affected by the attack were not actually protected behind any kind of firewall and the ones that had were weak and easily oppressed. As Lindqvist & Neumann (2017) stated, "we have weakness in depth and breadth, not strength in depth. Therefore, many problems will need to be overcome to make the IoT viable." (p. 27). The system, as a whole, needs to be carefully inspected to address all the potential vulnerabilities including, the devices, firewall security, network connectivity, cloud services, and the Internet, as we know it, will need some changes. We cannot view IoT as an entity because it depends greatly on all of these entities. It is possible this recent attack is simply a forerunner of imminent attacks. In the future, IoT attacks

will be pervasive, gaining trustworthiness to only compromise it later. Human safety, reliability, resilience, seamless ease of installation and use, and human well-being are just a few requirements that must be addressed networkwide (Lindqvist & Neumann, 2017).
The capacity to sabotage Things remotely for random manipulation must be considered particularly threatening. Lindqvist and Neumann provide some examples of application areas where the use of IoT devices brings inherent risks (2017):

- Hospitals and healthcare facilities can expose human life to a great risk with all the devices they use. Everything from patient monitors and infusion pumps to lighting and air conditioning could be attached which would be devastating to patients.
- Infrastructure that is critical, for instance, electric power, oil, gas and transportation all use IoT to automate and remotely control devices.
- Self-driving cars could be the scariest and most vulnerable industry since it's fairly new. Automobiles could be remotely hacked and controlled without the proper protections to prevent it.

Confronting the Risk

As already noted, risk for IoT must be considered in the setting of total systems. The security of Things is only one part and the system from top, down will need to be secured. First, consider the type of operating systems Things will use. Some will have the very basic which is essentially no operating system. Others may need a basic operating system that can handle specific task while the more complicated Things will need complete operating systems for demanding and complex processes. Since companies will have all these different levels of complexity, it will be much easier to have scalable operating systems that work with all applications. As a result, this will create similar development and programming languages that will only make it more plausible for someone to hack (Lindqvist & Neumann, 2017).
Things will be controlled by users that want these devices to be easier than ever to use. Making the user interaction as simple as possible while creating a fortress of security on the backside could create glitches and quirks that will need to be addressed. Fail-safes will be very important in this landscape. Consider a gas company that remotely controls certain processes in the refining production. What happens if they lose power in the middle of a crucial process that could cause disaster? Companies must be able to create proper fail-safes that will prevent such disasters.

BUSINESS IOT

Business Analytics

Companies are relying more and more on analytics to study their business and make improvements. Yerpude and Singhal (2017) describe analytics as this, "It is not a technology in and of itself, but rather, groups of tools that combine with one another to gain information, analyze that information, and predict outcomes of the problem solutions resulting into accurate and quick decision making." (p. 2). We are currently in Industry 4.0 which mainly revolves around automation. Things, meaning machines, sensors, and products, will only benefit from greater use and knowledge of analytics with IoT. The more understanding gained mean the better Things will direct, optimize and automate their decision-making (Yerpude & Singhal, 2017). Business

analytics cannot survive without the whole system being created. It becomes irreverent and insufficient without the proper investments which "includes the resource allocation and orchestration along with the necessary investments to build the same with the IoT framework and usage of the same." (p. 3). Without the proper IoT infrastructure, companies will not be able to take full advantage of quick and accurate decision-making.

Cloud

While cloud computing has already been in our lives for a while now, it will only become more pervasive and important as time goes on. Moving in the same direction but slightly lagged, is IoT. Botta, De Donato, Persico & Pescapé explain this phenomenon as a new paradigm called "CloudIoT":

The two worlds of Cloud and IoT have seen a rapid and independent evolution. These worlds are very different from each other and, even better, their characteristics are often complementary, as figure 1 shows. Such complementarity is the main reason why many researchers have proposed and are proposing their integration, generally to obtain benefits in the specific application.

	IoT	**Cloud**
Displacement	Pervasive	Centralized
Reachability	Limited	Ubiquitous
Components	Real World Things	Virtual Resources
Computational Capabilities	Limited	Virtually Unlimited
Storage	Limited or None	Virtually Unlimited
Role of the Internet	Point of Convergence	Means for Delivering Services
Big Data	Source	Means to Manage

Note. Referenced from Integration of Cloud Computing and Internet of Things: A Survey. 2015

Given all these complementary characteristics, we can see how IoT and Cloud can fill gaps where the other lacks. There are a few drivers that bring us closer to integration (Botta, De Donato, Persico & Pescapé, 2015). *Communication.* The Cloud brings a new solution to connect, track, and manage any data collected from IoT. It's a much cheaper alternative for companies to utilize for all their various products with internet connectivity. On the other hand, IoT provides the Cloud the capabilities to send data to devices at a low cost. *Storage.* IoT produces a very large amount of data that must all be stored. This data comes across in non-structured or semi-structured format and three different characteristics: volume, variety, and velocity. Cloud is the most convenient and cost effective way to store this mass of data. Once this data is there, it can be seen from anywhere by anyone that has the credentials to see it. *Computation.* "IoT devices have limited processing and energy resources that do not allow complex, on-site data processing." (Botta, De Donato, Persico & Pescapé, 2015, p. 12). Typically, data is sent to more powerful centers where it can be processed into valuable information but scalability has always been the challenge. Cloud can be used to eliminate that issue and be used on-demand. As soon as more storage is needed, it's as easy as flipping a switch. Another positive feature, is the data can be converted and sent back in real-time. *Scope.* As we continue to add capabilities, creating "CloudIoT", more and more Things will come online connecting more and more people with them. This concept will bring us into Internet of Everything (IoE) which is "network of networks where billions of connections create unprecedented opportunities as well as new risks." (Botta, De Donato, Persico & Pescapé, 2015,

p. 12). Every new paradigm, through innovation, will create new processes and ways to do business. Once that is achieved, essentially anything and everything can be possible.

Human Resources

During our time at work, which can be the majority of active hours, taking breaks is something important and IoT can now play a role in it. "Recent health research has shown that too much sitting, especially prolonged periods of sitting without breaks, is harmful for metabolic as well as musculoskeletal health, regardless of how much exercise one does." (Huang, 2016, p. 2). There are two key issues when encouraging regular micro-breaks at work. First, delivering the alarm in a manor that's not disruptive to others around or causing great annoyance to the user. Second, the availability of necessary devices that will monitor what the user is doing, report health reports, and help set goals. According to Huang, the answer to these issues could be in "Enchanted Objects" (EOs) for just-in-time health behavior change interventions in settings like the office (2016). EOs can be described as regular, everyday objects gaining power from embedded sensors, transmitters, and processors to interact with humans. Three qualities characterize what EOs can do: glanceable, gestural, enjoyable. EOs should be glanceable so that they are not disruptive, something that isn't noticeable except for the user in a slight manor. An example of this could be a popup or screen break. Gestural, meaning "their physical forms suggest actions in line with existing human skills and experience with those everyday objects." (Huang, 2016, p. 2). What good would EOs be if the user didn't enjoy them? Everything about the EOs should be create empowerment and support the user's needs. Who would have thought that IoT could play a huge role in improving the lives of employees? The paths are truly endless.

Marketing

In the future, IoT will become an impactful marketing tool for large firms. Currently, most consumers believe the average retailer does not understand them and about the same amount say marketing messages are not relevant to them. While retailers know, this must change, few believe they currently have the tools needed to provide exceptional customer service. (Gong, 2016). According to Gong, there will be four technologies that will be important for marketing success in the near future: Cloud computing and services, mobile solutions, IoT, and cognitive computing (2016). IoT will play a huge role in customer engagement and collection of data. As more Things become connected, marketers will have the ability to send signals or messages to their target customers. Those customers will be able to respond in some via message, clicks or purchases which is data the marketers will collect. We have seen the effect IoT can have at home with products like Nest, Siri on Apple TV, Amazon Echo, Phillips Hue, and Belkin Wemo but items similar to these will soon be available for applications outside the home. Manufacturers and Industries should be monitoring how this transformation has come to homes and find opportunities to bring them to business. IoT is going to revolutionize the way marketing is done. Home applications are only the tip of the iceberg and starting point for what businesses will be able to do. "It is expected that by 2020, the worldwide market for IoT solutions will be $7.1 trillion. The estimated IoT connected devices will be +13 billion by 2020." (Gong, 2016, p. 7).

The automobile industry is a good example of the future impact of IoT on Industry. Google has their self-driving cars which clearly demonstrate the possibilities but it's also known that

mainstream technology can take up to 3 years to impact the auto industry. We are starting to see cars get connected faster than before. You now have AirPlay, Android Auto, and Spotify available in your vehicle. Some cars even have the ability to provide Wi-Fi through mobile networks. Soon enough, they will not only be connected but they will be "smart". Detour indicators, traffic notifications via highway, and road signs will all be able to provide real-time updates in plenty of time to take alternate routes. Automobile leaders and software providers will continue to team up and deliver great value to consumers. Each having their own agenda for what the auto industry should and could be but either way, car buyers will reap the benefits.

Vertical Cooperation

As it currently exists, companies cannot have complex IoT solutions alone. They require resources and knowledge from different industry that help complete the ecosystem (Ghanbari, Laya, Alonso-Zarate, & Markendahl, 2017). With the need of others, relationships must be made in order to deliver to the customer. "There are four major categories for business relationships:

- Co-existence: firms exist and affect each other indirectly, without direct business interactions.
- Cooperation: firms interact with each other on a collaborative goal.
- Competition: firms compete over similar goals that directly relate to resources possessed by each firm.
- Coopetition: comprises competition and cooperation happening simultaneously.

These four categories fall within two major setups: vertical and horizontal." (Ghanbari, Laya, Alonso-Zarate, & Markendahl, 2017, p. 2). Cooperation and coopetition will continually become more important and crucial for companies. Developing new IoT products will be very challenging and by "going co-op" companies will be able to reduce transaction cost and handle resource dependency. (Ghanbari, Laya, Alonso-Zarate, & Markendahl, 2017). In order for this to happen, there will need to be new players from other industries in the IoT value creation process. Each company that enters the IoT value creation will have a vision and mission. They will be interconnected and dependent on each other. In the future, companies will need to understand how their own value chain is connected to the value networks created by IoT. (Ghanbari, Laya, Alonso-Zarate, & Markendahl, 2017).

5G Mobile Networking

"It is fair to say that it is still the early days for 5G" (Carlton, 2016, p. 1) but with cited requirements of 1000x improvement over LTE and huge reductions in end-to-end latency, 5G could mean big things for IoT. To put it in perspective, GSM (2G) only supported 9.6 kbps while LTE can, theoretically, support up to 960 mbps which is 100000x faster! That's only 20 years of cellular technology. Telecommunication companies will become more involved, cooperative and coopetition, once 5G is widespread. With 5G, a Wi-Fi connection is no longer needed, IoT can connect easier and send data faster without interruption. "This is the real 5G challenge, and in this respect 5G and the IoT are simply two sides of the same coin." (Carlton, 2016, p. 1). Exciting innovation and product improvement will be driven by the next generation!

Conclusion

Entering new horizons of IoT in more business practical applications is going to be exciting. Companies will adjust, mold and create based on this technology and for this technology. Jobs will be added and transformed to meet the needs. Consumers will receive marketing that is more accurate to their needs. Our business leaders will have more advanced tools at their disposal to guide their decision-making in uncharted ways. Business as we know it will forever be changed, good and bad, as IoT advances.

REFERENCES

Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. Future Generation Computer Systems, 56, 684-700.

Carlton, A. (2016). 5G is coming and it is the future of mobile. Network World (Online), Retrieved from https://0-search.proquest.com.ucark.uca.edu/docview/1762740521?accountid=10017

Ferber, S. (2013, May 07). How the Internet of Things Changes Everything. Retrieved March 19, 2017, from https://hbr.org/2013/05/how-the-internet-of-things-cha

Ghanbari, A., Laya, A., Alonso-Zarate, J., & Markendahl, J. (2017). Business Development in the Internet of Things: A Matter of Vertical Cooperation. IEEE Communications Magazine, 55(2), 135-141.

Gong, W. (2016). The Internet of Things (IoT): what is the potential of the internet of things (IoT) as a marketing tool? (Bachelor's thesis, University of Twente).

Huang, Y. (2016, September). How to Design Internet of Things to Encourage Office Workers to Take More Regular Micro-Breaks. In Proceedings of the European Conference on Cognitive Ergonomics (p. 32). ACM.

Lindqvist, U., & Neumann, P. G. (2017). The Future of the Internet of Things. Communications Of The ACM, 60(2), 26-30. doi:10.1145/3029589

Morgan, J. (2014, May 13). A Simple Explanation Of 'The Internet Of Things' Retrieved April19, 2017, from https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#7fa6ecd01d09

Wu, D. J., Taly, A., Shankar, A., & Boneh, D. (2016, September). Privacy, discovery, and authentication for the Internet of Things. In European Symposium on Research in Computer Security (pp. 301-319). Springer International Publishing.

Yerpude, S., & Singhal, T. K. (2017). Internet of Things and its impact on Business Analytics. Indian Journal of Science and Technology, 8(1).