Internet of Things:
An interconnected physical and digital world

Michael Wang
Stony Brook University

Thesis Statement

The Internet of Things (IoT) function is communicating with many users and processing large amounts of data securely. Its impact is determined by its implementation in conjunction with cloud computing, cybersecurity, and machine learning.

Literature Review

Computers complete tasks better than humans because they are quicker, more accurate, consistent, and available. However, computers are not intelligent or self-aware like humans. Machines will only complete tasks assigned to them and because it is impossible to account for every sequence of tasks, human interaction is necessary. The IoT is a system that facilitates human-computer interactions, making it easy for users to delegate tasks to computing devices. The fundamental idea of the IoT is that a user of any internet thing can access that device anytime and anywhere, directly or indirectly (Kulisz et. al 42). Likewise, the internet thing is able to communicate with their user from any location anytime. Intelligent shirts are used to monitor patients' ECG, pulse, temperature and blood pressure in Spain (Kulisz et. al 43). If the shirts were unable to communicate that information from any location, nurses would be limited to the same vicinity as the patient to view the information. The shirts are convenient because they communicate patient status through the internet, making them part of the IoT rather than a local tool.

The information sent by internet things like the shirts is collected and analyzed. That information scales to a huge amount with a large number of devices. For that reason, cloud computing is a perfect environment for the implementation of the IoT (Kulisz et. al 44). A reliable system for IoT applications should never fail, therefore IoT systems must be capable of handling huge spikes in internet traffic if necessary. However, paying for such expensive hardware is unnecessary considering the network will not always have peak traffic and make use of its potential. Instead, a company can pay for cloud computing resources on-demand, paying only for how much computing power is used. Cloud computing services fall into three main categories: infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). IaaS concerns the provision of software and hardware components. An IoT networking

infrastructure can be built with these components and sharing the same infrastructure across several applications is cost-effective (Bak et al. 914). Companies that use IaaS cloud resources should optimize their design to use the cloud resources in an effective and cost-efficient manner.

To determine the most effective design for an IoT system, designers need to determine if their application needs to be real-time. An example of a real-time interaction is a phone call, the communication needs to occur quickly. A navigation application that keeps track of cars using GPS and redirects them to the most-efficient route needs to be real-time. A centralized system is not be quick enough to process the huge amount of information in a reasonable amount of time. Real-time applications can be optimized by building a distributed network, or a network composed of layers (Bak et al. 923). If the car application was designed for a city, then the city should be partitioned into individual sectors that manage their own routes and pass that information along when a car changes sectors. When applications are not real-time, speed is not so important, so the application should have a cost-efficient design. The efficiency can be gauged by analyzing the amount energy lost or wasted (Mastelic et al. 33:5). Energy loss refers energy used for a purpose but lost in the process, internet packet loss would be an example of this phenomenon. Energy wasted refers to redundant tasks. Energy waste is a huge concern for buyers of cloud computing services because they want to minimize how much they pay for processing power. Applications should only communicate when necessary. The intelligent shirts in Spain could be optimized by only sending changes in a patient's status over the network, instead of constantly sending that information. Insignificant changes should also be eliminated to make the system even more efficient. If a patient's temperature changes by an insignificant amount, it is unnecessary to communicate the change. Efficiency is really important because IoT applications need to be scalable, small flaws in design become big flaws in a large-scale environment.

Since the IoT uses the internet to communicate information between devices and users, cyber-security is a giant determining factor of its success. There are several categories of attacks on wireless networks: confidentiality, integrity and availability (Borgohain et al. 2373). Each type of attack hinders the reliability of the IoT, limiting its applications to managing unimportant tasks. An attack on confidentiality accesses private information that is normally not available to unauthorized parties. Such information can include social security numbers and credit card number. The inability to secure the IoT from this type of attacks forces the IoT to manage tasks that do not handle personal information. Attacks on integrity refer to manipulation of data in a system, causing the information sent by devices to be unreliable. In such cases a person would rather complete a task without a machine. The most common attacks on availability are denial-of-service (DoS) attacks. DoS attacks can occur across physical, link, network, transport and application layers (Borgohain et al. 2373-2376). Each DoS attack acts on a particular layer to make the service unavailable. Failure to secure the IoT against these attacks limit it to tasks that are not urgent. The IoT allows provides a type of omnipresence to users and their devices, but cyber-attacks eliminate those benefits. In order to create a reliable IoT, there should be a large investment in the prevention of cyber-attacks.

The IoT has the ability to use machine learning algorithms for detecting trends and optimizing technology for user compatibility. If users and machines constantly interact through the internet, a lot of behavioral information is generated. A piece of technology that can communicate what features are often being used is able to assist product managers in determining which features to further develop. Statistical data is one of the greatest benefits the IoT provides. There are fitness bracelets that can survey fitness levels of individuals in respect to their lifestyle, gender, age and various other factors (Earley 12). However, these examples involve humans

identifying possible trends and confirming them. With machine learning technology, the IoT has a lot more potential than simply providing statistics. The IoT applications particularly useful in epidemiology because they can make predictions based on patterns in data (Earley 12). Machine learning algorithms can identify individuals struggling with depression by comparing their behavior with others afflicted and informing these individuals to get help before their condition worsens. Humans might not realize their peers are suffering with depression because they cannot constantly monitor their peers the way machines can.

The effectiveness of the IoT is determined by how it utilizes cloud computing, cyber-security and machine learning resources. As a stand-alone system, the IoT is not very impressive. Without good cyber-security, the IoT is vulnerable to internet attacks and without machine learning algorithms, it does not make full use of the information passing through its network. The usefulness of the IoT depends on how many human tasks have been simplified through human-computer interactions. The magnitude of tasks that is delegated to machines directly correlates with how efficiently machines can handle tasks and how comfortable users are with providing the information necessary to complete these tasks. Therefore, the usefulness of the IoT depends on the efficiency of cloud computing resources, cyber-security, and the opportunities machine learning algorithms provide.

Bibliography

Monika Kulisz and Jakob Pizon. 2015. “The Application of Cloud Computing with the Internet of Things”. *Applied Mechanics and Materials*, 791: 42-48.

Slawomir Bak, Radoslaw Czarnecki and Stanislaw Deniziak. 2013. “Synthesis of real-time cloud applications for Internet of Things” *Turkish Journal of Electrical Engineering & Computer Sciences*, 23: 913-929.

Toni Mastelic, Ariel Oleksiak, Holger Claussen, Ivona Brandic, Jean-Marc Pierson, and Athanasios V. Vasilakos. 2014. “Cloud Computing: Survey on Energy Efficiency”. *ACM Computing Surveys*, 47 (2): 33:1-33:36.

Tuhin Borgohain, Uday Kumar and Sugata Sanyal. 2015. “Survey of Security and Privacy Issues of Internet Things”. *Int. J. Advanced Networking and Applications*, 6 (4): 2372-2378.

Seth Earley. 2015. “Analytics, Machine Learning, and the Internet of Things”. *IT Professional*. 17 (1): 10-13