Security in Internet of Things

PhD Proposal

## 1. Introduction

The Internet has evolved over time creating more utility and value to the global society. According to [1], the Internet stated as a "Internet of Computers" in which only the electronic devices were connected to each other. As evident in the initial project that created internet, the aim was to share information in the research and business communities. At that time, the World Wide Web and other services played a more central role. However, it later emerged that there was need connect people to each other. As the original World Wide Web platforms were transformed into Web 2.0, it became the "Internet of People". This was characterized by people creating content while others consumed it. The best examples are offered by social media. It is estimated that the "Internet of People" is comprised of about 1 billion people.

A number of factors have led to the exponential growth on the Internet. [2] observes that broad band internet has increasingly become cheap hence affordable even for people in the developing countries. Other technologies and service provision approaches such as the fiber-based internet has led to increased use of the same. Companies such as Fiber Optic, SEACOM and EASSy have propelled this growth through their services [3]. In addition, technology companies manufacturing mobile devices have invented device that have higher processing and storage capabilities, things that are associated with the expansion of the internet of both computers, people and device. In a special way, the uptake of smart phones will continue to spur growth of the Internet. Needless to say, there is immense shift from the PC-based access to internet as was the case before. Tablet computers, notebook computers and related devices motivate more use of the internet. The speed of these devices, coupled with newer technologies of continuous data collection, such as the use of sensors and actuators, have introduced many "things" on the traditional Internet [4]. Being part of the internet of these things was based on the fact that they act "intelligently" such as the execution of a command by a smart phone or BR-code reader if they sense or read information tagged on physical objects. This inclusion of physical entities on the cyberspace led to the birth of the word "Internet of Things" (IoT) [5].

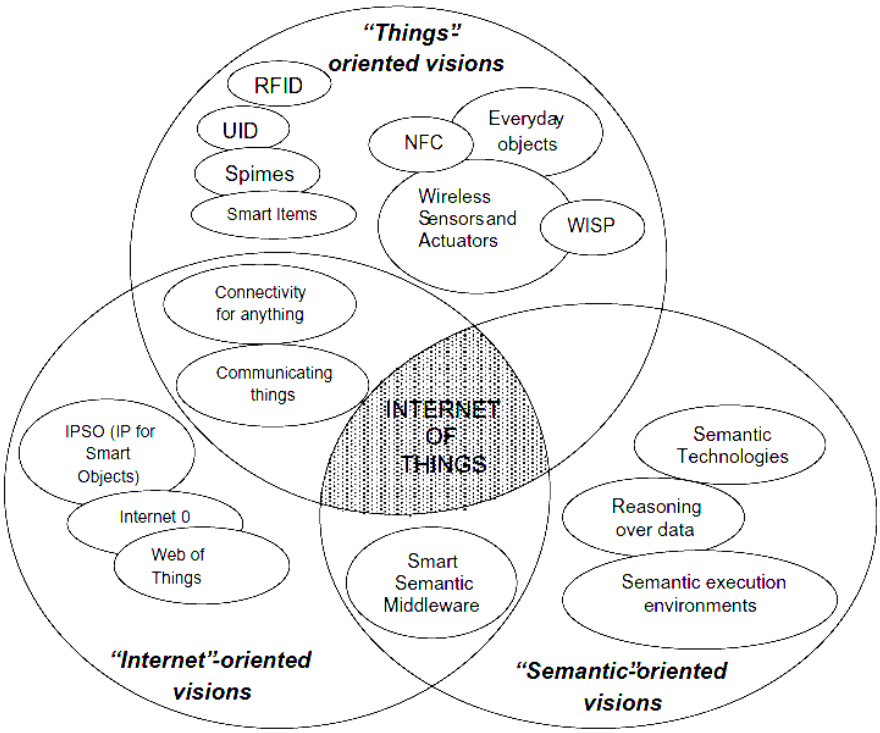
According to [4], IoT describes a vision in which things or objects become part of the internet. These things are uniquely identified and are accessible to the network. The International Telecommunications Union (ITU) described four characteristics of the "things" that make up the IoT. These characteristics; thinking, feeling, tagging and shrinking, make the things "intelligent" components of the IoT. Tagging is a dimension for item identification, thinking a dimension of embedded systems and thinking a dimension of wireless sensors. It is crystal clear that once the things are available on the network, more services can be rendered to the economy or the environment. However, [3] notes that some of the devices that are plunged into the networks that make up the Internet are malicious in their "thinking". Many examples exist of instances where applications were used to make trials in "guessing" a person's password [1]. In addition, as more things are introduced in the internet, more data is stored and the need to access the data by unauthorized entities created [2]. More significantly, since most owners of devices on the networks do not have technical training, they leave out many chances for third party attacks [5]. Failure to know how to change default settings while connecting to a network poses serious risks and vulnerabilities to the data. It is on this basis that security on the IoT becomes a pertinent issue in the present times as the "Future Internet" unfolds [5]. This study describes the

vulnerabilities and risks associated with peer-to-peer technologies in the IoT and proposes some security measures that can be undertaken.

## 2. Literature review

The concept of the IoT is rapidly becoming popular in the information and communities technology field. There are many definitions of IoT, but there is general agreement that its underlying concept encapsulates the presence of objects or things around us which can interact with each other through different schemes of addressing [7]. Examples of such objects or things include sensors, mobile phones, Radio Frequency Identification (RFID) tags, actuators among others. Different scientific communities have different visions of the IoT. [2] proposes a paradigm that consolidates all the possible visions of IoT as well as their enabling technologies. The author admits that some scientific communities, in visioning IoT, are more oriented towards the "Internet" part while others are more oriented towards the "Things" part. Admittedly, the orientation of the authorities in any scientific community forms the basis of the definition of IoT.

**Figure 1: The IoT paradigm as a consolidation of different visions**



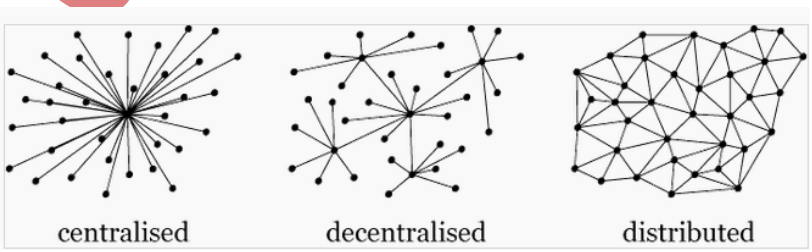

Source: [2] pg 2789

Although the use of IoT devices is on the increase, several security and privacy challenges are presented. According to [8], these are the major hindrances to the deployment of conventional IoT at the global scale. Although the present-day Internet is characterized by almost homogenous devices (mostly computers) with huge processors, memory and storage, the IoT environment is the exact reverse. Devices in networks that make up IoT are relatively slow compared to the ones on the conventional Internet. The IoT devices are supposed to share information via wireless networks. For instance, e-health applications on the IoT must be driven by quite sensitive data

about clients which, if leaked to third parties, or eavesdropped, may lead to serious consequences. One of the proposed approaches towards meeting the security challenges that come with IoT is giving a decentralized model in which devices must not be connected to the cloud by can share the information directly with each other [6] [7]. Model decentralized system has been created by BitBay and, as [8] notes, there is no single instance of failure or vulnerability. However, the BitBay platform is only for the purchase of goods and services via the internet.

[9] provides more detailed approaches to the enhancement of IoT security. It is observed that devices that are linked in IoT are characterized by sensors. As a security measure, there is need for all sensors to be authenticated in a bid to establish the origin of information. It is also required that not every person can access sensor data. In order to mitigate this, it is important that all requests that are made to access the data are authenticated. Admittedly, most of the security challenges faced on the internet are also faced on the IoT. For example, eavesdropping is a common security challenge that IoT networks must contend with. Therefore, anti-eavesdropping measures must be implemented as well as encryption. In securing the data transmitted through the IoT, there is need to implement secure point-to-point connections, a basic tenet of IoT as contrasted with the Internet. [6] recommends that infrastructure for IoT should take into account techniques such as identification, minimization, authentication and anonymity of data. Furthermore, as earlier pointed out, access must be controlled just as it happens in real world, through self-configuration and fine-graining. It is reiterated that end-to-end authentication is a key pillar to security on IoT.

Peer-to-peer (P2P) communication is understood as the direct communication or transmission of information between or among devices [10]. Some authorities have argued that even if IoT is not Internet per se, it uses the same principles as internet does. This is demonstrated by the fact that the Internet of people and PCs uses servers while P2P communication, one of the bases for IoT, has nodes that serve this purpose. It is observed that the nodes in a P2P communication arrangement do a variety of things as the same node; such as client, “server” that responds to other nodes, requester of web services as well as provider of resources and services to other nodes. According to [6], networks are either distributed, centralized or decentralized. Since the IoT seeks to be different from the traditional Internet and the telecommunications, it adopts a decentralized model.

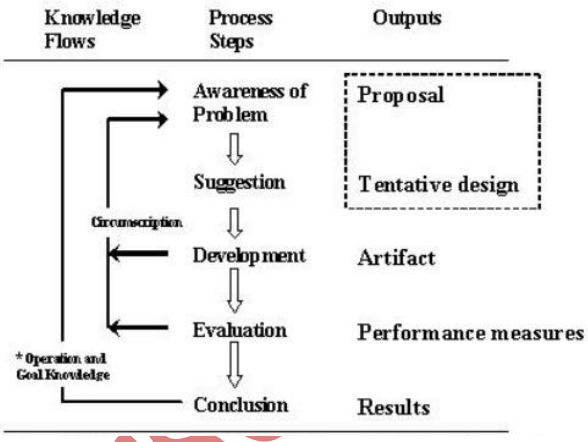



A good example of a decentralized model in the modern times is the BitBay. It is an online marketplace that enables people to buy and sell things to anyone anywhere with no slightest level of vulnerability. According to [8], payments are guaranteed. This was possible though what they referred to as BitBay Wallet that enables the creation of Smart Contracts. All the functions on the marketplace are decentralized and are determined by the decisions of the users. Through the Wallet, users can check their balances and even save money.

Although decentralized designs are the ideal for IoT, there are hurdles related to the same. One of the hurdles is the emergence of big data [9]. This does not imply that IoT does not need or generate big data, but has an implication on the storage of the collected data. This further implies the need for cloud computing, a concept that works very well with the traditional internet. This is because instead of devices exclusively linking to each other, they begin to link to the cloud as before. This led to [7] arguing that cloud computing could lead us back to the centralization of networks of things. In order to overcome this challenge, [7] proposes the use of a Filament Tap that gives APIs.

## 3. Methodology

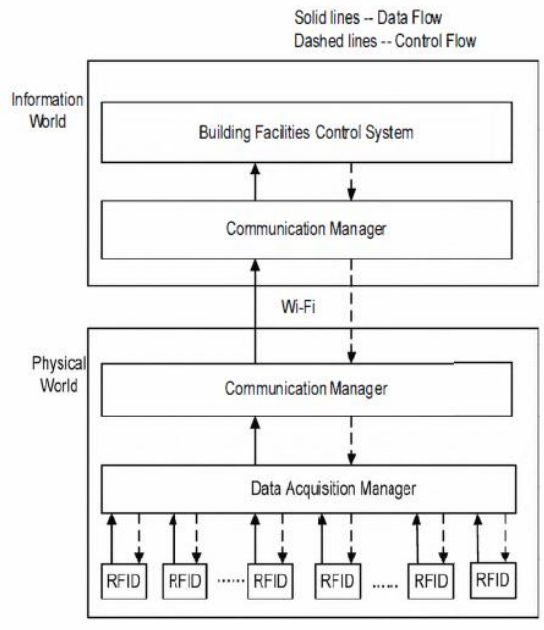
The aim of this section is to propose an approach through which the centralized model of networks can be solved. This can easily be achieved through design science [11]. The general methodology for all the design research is represented below.




As the above figure shows, the general methodology is to apply process steps on established knowledge flows (of the centralized system) to produce outputs (decentralized design). For each step of the process, corresponding outputs are provided. The steps are as follows: awareness of the problem, suggestion, development, evaluation and conclusion. The outputs for each of the process steps are: proposal, tentative design, artifact, performance measures and results. For this study, the IoT will be used to analyze the facilities at the college campus.

The college has several facilities such as the lecture rooms, administration block (offices), library among others. Each of the buildings has its own facilities such as heaters, ventilations, air conditioning (HVAC) and elevators, but managing the devices is not easy. The IoT technology can be used to manage the facilities as envisaged on the schemata below.

**Figure 2: Architecture for the management of facilties in college campus**




Specifically, each physical equipment will be fixed with a RFID tag that will not only collect information continuously but also sense the changes that occur within the physical environments of the equipment such as wetness and the like. Since the campus has Wi-Fi, data collected by facilities manager in each building will be transmitted to control system of all the facilities. The communications manager or the person in charge will interface the physical and the information worlds. Later, the system carries out the analysis and makes decisions regarding each of the facilities and its components. For instance, some air conditioners could be turned off, it the conditions are on the extreme. All this can be effectively done without human intervention.

## References


[1] L Tan and N Wang. Future Internet: The Internet of Things. 2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE), 2010.

[2] L Atzori, A Iera and G Morabito. The Internet of Things: A Survey. Computer Networks 54, 2010.

[3] JA Stankovic. Research Directions for the Internet of Things. IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 1, FEBRUARY 2014.

[4] L Coetzee and J Eksteen. The Internet of Things- Promise for the Future? An Introduction. *IIMC International Information Management Corporation, 2011*.

[5] J Rivera and R van der Meulen. Gartner Says the Internet of Things Will Transform the Data Center, March 19, 2014. http://www.gartner.com/newsroom/id/2684616

[6] J Webb. A vision of a decentralized IoT stack, May 10, 2015. http://radar.oreilly.com/2015/05/a-vision-of-a-decentralized-iot-stack.html

[7] J Evans. Decentralize all the Things, Jan 10, 2015. http://techcrunch.com/2015/01/10/decentralize-all-the-things/

[8] N Menezes. BitBay – Decentralized Marketplace and the Internet of Things, November 20, 2014. http://bitcoinist.net/bitbay-decentralized-marketplace-and-the-internet-of-things/

[9] AF Skarmeta, JL Hern´andez-Ramos and MV Moreno. A decentralized approach for security and privacy challenges in the Internet of Things. IEEE World Forum on Internet of Things, 2014.

[10] J Gubbi, R Buyya, S Marusic and M Palaniswami. Internet of Things: A vision, architectural elements and future directions.

[11] X Cheng and G. Dang. The P2P Communication Technology Research Based on the Internet of Things. IEEE Workshop on Advanced Research and Technology in Industry Applications, 2014.