**PAPER TITLE**: IOT -DATA COMMUNICATION SERVICES IN CLOUD

**COURSE TITLE**: DATA COMMUNICATION &DISTRIBUTIVE DATA PROCESSING

**AUTHOR NAME**: SANDEEP KUMAR CHINTALAPALLY

**DATE**: June 23, 2017

**EMAIL ADDRESS**: [SXC96520@UCMO.EDU](mailto:SXC96520@UCMO.EDU)

**Introduction**

The IoT (Internet of Things) technology changed the current networking communications. Currently any electronic device can communicate with other devices via different network data communication protocols. The main aim of IoT technology is to predict the life time of IoT enabled devices based on the data that are collected from remote devices. While the data is playing an important role in IoT technology, how IoT addresses the security challenges while data is collected via network communications. This paper describes the security risks associated with IoT services and solutions offered by Microsoft Azure (Marsan, 2015).

**How the Data is collected**

There are two basic communication models that are widely used to collect the data from different devices.

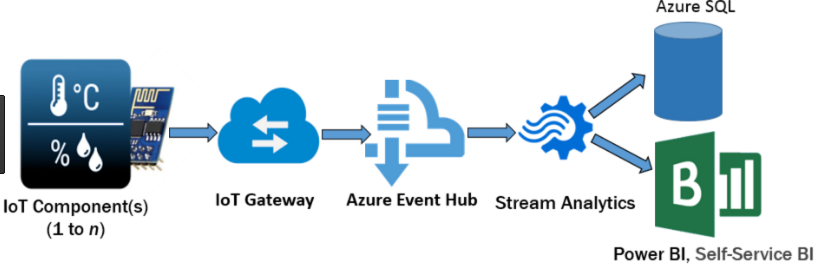
1. Device-To-Device Communication Model
2. Device -To-Cloud Communications Model
3. **Device-To-Device Communication Model**

 Iot enabled light Switch

Wireless (Blue tooth)

This DTD communication model represents two or more devices connect each other via IPv4 protocols, Bluetooth and Z-wave. This type of communication model uses to build the home automation systems, where it requires to transfer small amount of data over the Bluetooth enabled protocols.

1. **Device-To-Cloud Communication Model**



The IoT components will sense the data from different sensors and transfer the data to IoT gateway. The IoT gateway will validate the device authentication and sends to the Azure event hub, based on event type, respective stream analysis will perform analysis and store in data repositories (Furness, 2017).

**What are the Security challenges in IOT?**

The principle will set the base line of working process and same principle must ensure that Security, reliability, resilience and stability of the internet of things. Trust full data is always is the important factor and that’s what user needs to know about the remote devices. If there is any fault data then the user may lose the confidence on the working system of IoT.

**Case Study 1**

April 7,2017 Dallas, the internet hackers turned all the emergency sirens at once, its created an emergency that entire city was in red alert. This incident happened because the siren devices are associated poor network security layer. Hacker injected false data to sirens which responded unauthenticated data.

The case can be rectified by using one of the IoT intelligent device authentication using Microsoft IoT hub. Where each device must be authenticated before sending the data to remote device. Azure IoT hub has matured service that enables greater security using X.509 certificates where each device must be authenticated before data need to be sent to back end systems. There different certificates that Azure IoT supports.

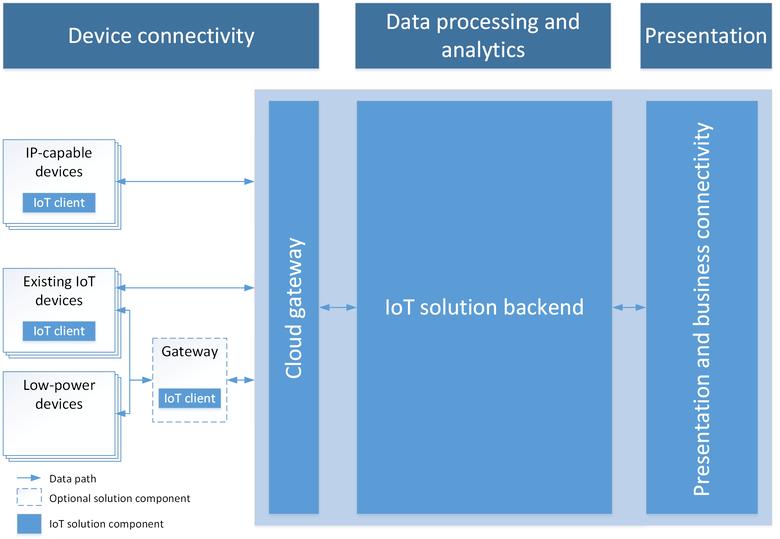
**An Existing X.509 Certificates:** The device installed with X.509 certificate which unique key for that device which needs to be encrypted while sending the data to IoT hub where the key will be validated.

**A self-signed Certificate:** The device manufacturer will generate these certificates while manufacturing device and these certificates associated with valid expiration date and other meta data which can help full to identify the device in a big network uniquely.

**Microsoft Azure IoT Security Solutions**

Azure IoT hub provides Secure communication per-device and Multiple-devices-cloud and hyper scale communications.

**Microsoft IoT Hub Archtecture**



The IoT devices are sending the data to the gateway where all devices can authenticate and transform the raw data into stream and save it cloud repositories. Each IoT device enabled new innovations to read the real-time data using secured channels and analyze the behavior the device (Betts&Berdy, 2017).

**Artificial Intelligence Security in IoT:**

Today, the security systems authenticated based on two elements in the world. First is human where they uniquely identified using bio-metrics processes and secondly machine where they can be identified using Machine IP addresses. Machine learning can enable behavioral based approach to protect IoT devices securely. The approach here is that using machine learning algorithms the data can be analyzed and identify the common behavioral part and record the device data pattern. If any data which is not match with recorded pattern then the data packet recorded as threat packet and stop responding to the respective sender(Dickson,n.d).

**Microsoft Azure Security Use Cases IoT**

Microsoft Azure IoT hub addressed the basic security issues that are associated with device authentication and device authorization. It’s used in different industries like Health care, wearable sensors and manufacturing (Algorithms.io, 2016).

As a conclusion, the world is going to connect 4 billion devices over the internet to function the services and operate the all devices. Though, the security became major concern, the current technology will replace the security concerns and bring an innovation where each human can talk to all devices securely using different data communications protocols.

**REFERENCES**

Algorithms.io. (2016). *Machine Learning for Streaming Data.* Retrieved from www.Algorithms.io

Betts, D., Kshirsagar, D. & Berdy, N. *Overview of Event Hubs Dedicated*. MICROSOFT. 16 June, 2017, https://docs.microsoft.com/en-us/azure/event-hubs/event-hubs-dedicated-overview

Betts, D., Kshirsagar, D. & Berdy, N. *Overview of the Azure IoT Hub service*. MICROSOFT. 16 June, 2017, https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-what-is-iot-hub

Dickson, B. “Machine learning will be key to securing IoT in smart homes.” *IOT Security Foundation*, n.d, /iotsecurityfoundation.org/machine-learning-will-be-key-to-securing-iot-in-smart-homes/

Furness,D. “An AI Cybersecurity System May Detect Attacks With 85 Percent Accuracy.” Techemergence, www.techemergence.com/an-ai-cyber-security-system-may-detect-attacks-with-85-percent-accuracy/ 19 April, 2017.

Madakam, S., Ramaswamy*,* R. & Tripathi, S. (2015)*. Internet Of Things (IOT): A Literature Review: Journal Of Computer and Communications, 3, 164-173.* http://dx.doi.org/10.4236/jcc.2015.35021

Marsan, C. (2015). *The Internet of Things: An Overview.* Reston, USA: The Internet Society

Simons, A. *System predicts 85 percent of cyber-attacks using input from human experts*. MIT, 18 April, 2016, http://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418

Yue, Xu. “Recent Machine Learning Applications to Internet of Things”, 30 November, 2015, http://www.cs.wustl.edu/~jain/cse570-15/ftp/iot\_ml.pdf