OULU UNIVERSITY OF APPLIED SCIENCES

Katunzi Bernard Rwanshane

STRUCTURE OF TYPICAL IOT SETUP

STRUCTURE OF TYPICAL IOT SETUP

Katunzi Rwanshane
Bachelor's Thesis
Autumn 2016
Information Technology
Oulu University of Applied Sciences

ABSTRACT

Oulu University of Applied Sciences
Information Technology, Option of Internet Services

Author: Katunzi Bernard Rwanshane
Title of the bachelor's thesis: Structure of Typical Internet of Things Setup
Supervisor: Kari Jyrkkä
Term and year of completion: December 2016 Number of pages: 29

The aim of this thesis was to research and study about Internet of Things architecture by identifying a model architecture and explaining the different technologies applied in the architectural model.

Secondly the security of Internet of Things was discussed based on the architectural layers and a number of Internet of Things use cases were explored.

As a result, this thesis can be used as a basis for identifying and categorizing the different technologies that are used in different Internet of Things application scenarios.

Keywords: IoT, internet Protocols, Internet of Things security, IoT Architecture, IoT Application scenarios, internet of Things structure.

PREFACE

This thesis was written for Oulu University of Applied Sciences from 1st August to 15th November 2016. A number of people facilitated the writing of this thesis, including the author who did an extensive research to identify concrete material for the thesis and the supervisor who revised and approved the thesis plan and cross checked that the thesis requirements were met.

Oulu 21.10.2016
Katunzi Bernard Rwanshane

TABLE OF CONTENTS

VOCABULARY

- IoT Internet of Things
- OSI Open Systems interconnection
- TCP Transmission Control Protocol
- IP Internet Protocol
- RFID Radio Frequency Identification
- WSN Wireless Sensor Network
- MAC Media Access Control
- EPC Electronic Product Code

1 INTRODUCTION

The ‘Internet of Things’ terminology has been gathering a lot of attention the past years. For example, from Google Inc. buying Nest labs for 3.2 billon dollars to new phrases like smart homes, smart cities, smart industries and new developments ranging from people being able to control and track things from a distance, self-switching home lights to self-driving cars, have all become possible. But what is IoT exactly?

The title Internet of Things can be traced back to the presentation made by Kevin Ashton at Procter & Gamble in 1999. He stated, that the Internet of Things is giving computers the ability to see, smell and hear things in the world without human help. With the data collected, things can be tracked extensively [4]. Hence, humans can know the complete status of these things, for example do they need repairs, treatment or how to improve the output of machines in a factory and many other scenarios.

Internet of Things is a diverse concept with no common definition of what it actually is. It is complex and is being applied in many different ways to different aspects of life, for example factories, military purposes, health science and many more. Therefore, to have a common structure is a challenge. However, with this thesis the root of an IoT architecture, which can go on and have many forms depending on where and how it is being applied, is explained.

2 KEY PLAYERS IN A TYPICAL IOT APPLICATION SETUP

As the Internet of Things is a new phenomenon, its architecture is still up to debate. Currently there are two widely accepted architectures of the Internet of Things. The first one is a EPC Global based “Internet of Things” architecture supported by Europe and the United States. It consists of an EPC encoding system, a radio frequency identification and an information network system. The second one is The Japanese Ubiquitous ID (UID)(IoT) system involves a ubiquitous identifier, a ubiquitous communication device, an information system server and ucode analysis servers. [2]

We can identify and group key players in a basic IoT set up using a newly established architecture based on the TCP/IP model. This divides IoT into generally 3 layers: An Information Perception layer (sensors, RIFD), data exchange/transport/network layer (networks and protocols) and an information application layer (cyber physical systems). [1][3]. By understanding the different layers put forward in this architecture and using it as a template, we can identify the key players in an IoT setup. (See figure 1)

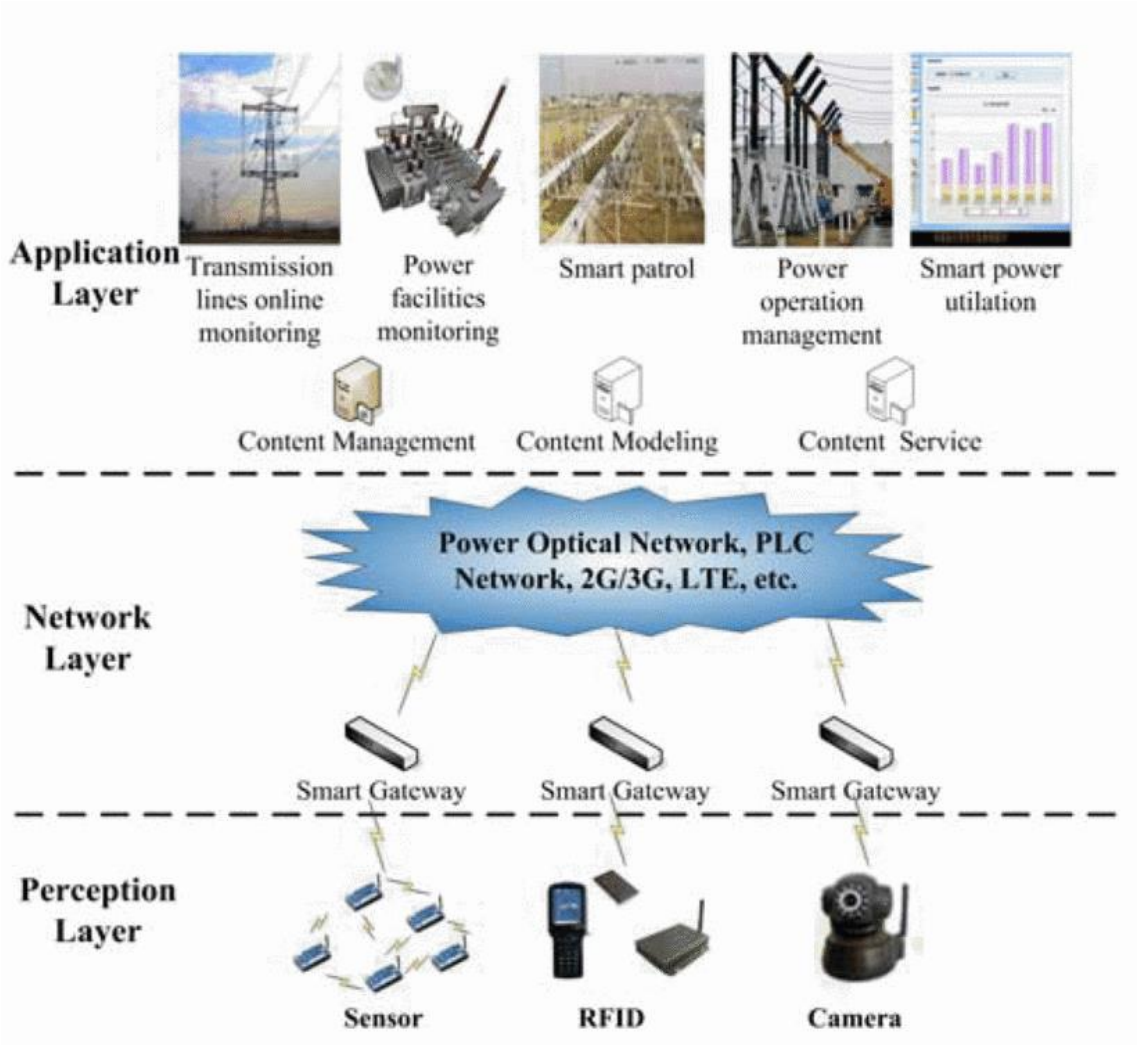

FIGURE 1. IOT Architecture (11)

2.1 Perception layer

Perception layer, also known as the device layer consists of physical objects and sensor devices such as two-dimension code tag and a code reader, a radio frequency identification, camera, a GPS, all **kinds of sensors**, a sensor network, a M2M terminal and a sensor gateway et al. The main function of the perception layer is the perception and identification of objects and collecting information. (2).

This layer basically deals with the identification and collection of objects specific information by the sensor devices. Depending on the type of sensors, the information can be about location, temperature, vibration humidity or chemical changes in air. The collected information is then passed on to the transport layer. [3]

2.2 The Transport layer

Transport layer is responsible for transmitting the data received from the perception layer to application layer through various networks, for example **wireless or cable networks.** The main technologies used include 2G, 3G, Bluetooth, infrared depending upon the sensor devices [3] This layer also includes many **protocols** which govern how the information should be lined up for transfer, how it is transmitted and how it should be received. Because data/information is transferred across long distances through all kinds of networks that employ different kinds of technologies, protocols are needed to ensure that data is smoothly sent and received and what to do in case of errors.

This layer handles the transfer of data to places where it can be processed and manipulated.

2.3 The Application Layer

Acquiring, storing, analysing and processing of data received from the transport layer is done in the application layer it involves to name a few, **cloud computing**, **ubiquitous computing**, **intelligent processing** and **mega databases**. With these technologies vast data is analysed and tailored for a specific purpose hence **data analytics**. [3] It is then made available for all kind of use.

The processed information is then used by different industries to achieve different goals for the end user. For example, through the creation of applications that make use of the data, in manufacturing industries data of the manufacturing process is used to track machine functionality (in case of need of maintenance).

3 PERCEPTION LAYER TECHNOLOGIES

This layer involves the gathering of information and identification of objects that are gathering information. Information gathering was once a human only phenomena but with IoT it is possible for objects to gather information on their own without human input. This is possible with sensors attached to the ‘things’, i.e cameras or GPS. As these ‘things’ are gathering information, they need to be identified with technologies such as RFID or a bar code reader.

3.1 Sensors

Sensors are the measuring tools for different kinds of perceivable things in the environment and these range from the temperature and humidity, to height, finger texture for fingerprints and many more. [8]

Sensors have greatly decreased in size over the years reaching a point where they can be easily fitted to small everyday things such as mobile phones and watches, creating a greater opportunity for collecting data hence the fact that IoT is associated with a large amount of data.

Some devices do not only have sensors but also actuators thus as they can react to the data they collect these are called embedded systems.

3.2 RFID Technology

The ‘things’ that collect data need to be identified and this can be done with the Radio frequency identification system, simply know as RFID.

In a typical RFID set up an object or objects are equipped with RFID tags (responders) so that they can carry out operations such as counting and they can be identified. The responders are made up of a microchip and an antenna.

The RFID setup also have RFID readers (receivers) which collect data from all RFID tags that are in its radio wave range and share the data with an application software. By doing this the RFID reader can identify, track, monitor and in

some occasions invoke reactions from objects with RFID tags within its range by sending energy waves to the tagged object. Figure2 shows an RFID setup structure. [9]

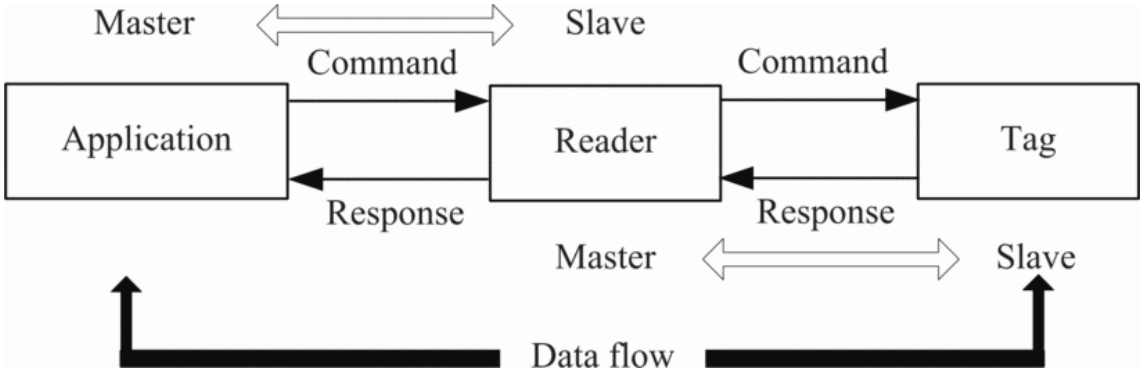

FIGURE 2. The components of a RFID system [9]

3.3 Wireless Sensor Networks (WSN)

In the perception layer there can be all kinds of sensors in a closed environment collecting different kind of data forming a network of sensors. These sensors are usually connected wirelessly to form a wireless sensor network, for example at home there can be a wireless sensor network of home appliances including fridge, televisions, coffee makers, or door sensors which collect all kind of sensory data and send it to a central processing unit for analytics. [15]
A technology that could be used to facilitate a wireless network of sensors is ZigBee.
ZigBee Utilizes low radio frequency to facilitate the connection of sensors hence forming a ZigBee network. A typical ZigBee network can consist of ZigBee devices which can be everyday objects with sensors, and a ZigBee coordinator which collects and directs data to a computational central system as illustrated in the figure 3 below [16]

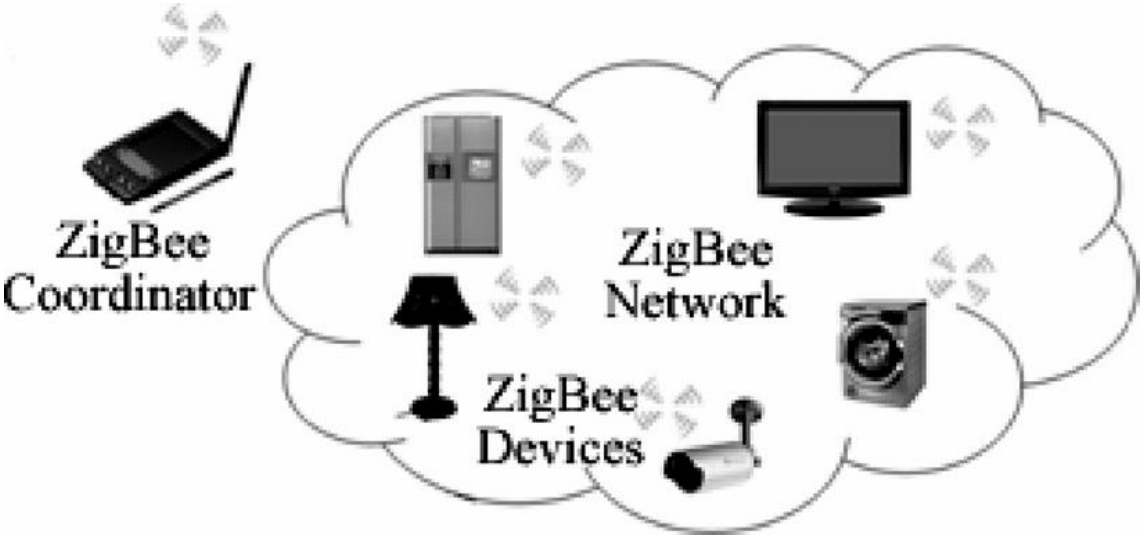

FIGURE 3. Sketch of a typical ZigBee network of sensors setup [16]

4 TRANSPORT LAYER

The Transport layer is the most mature of all the three layers since it has been around for some time and has been thoroughly researched and documented, It is made up of infrastructure that facilitates the connection of things either locally or on a wide geographical area both physically through optical cables or wirelessly through different technologies, such as 3G, and protocols that govern how information and data is exchanged between end points in the layers or while in transit through different networks,

4.1 Networks

In order for data to travel from the place of perception to the end user or computational and storage centres, the communicating devices need to be connected leading to the formation of heterogeneous networks with different structures spanning different geographical areas, where a wide range of technologies are in place to ensure that different devices can interact with one another seamlessly Some of the technologies applied to wide area networks include eg. 3G/4G cellular communication technologies, Wi-Fi, satellite technology. A common example of a network is the Internet.

In a general network set up a network begins as a single node which is connected to other sensors to form a network of sensors either through wires or wirelessly Then this network of nodes can be connected to other networks of nodes to form a local area network of nodes for example in an office building or at the premises of a factory through Wi-Fi or physical connections by wires. These Local area networks will continue growing to form wide area networks of devices and data centres.

4.1.1 Network categories

Networks can be categorised based on a number of factors that range from the geographical area served to the type of medium used for data transmission (wired or wireless) et al. Below some of the categorises are explained briefly.

Based on network packets: Networks can be categorised based on the fact that they support network packets (Packets are a formatted unit of data.) or they do not. networks that do not support packets are called circuit switched network.

Based on the Medium of transport. Data is either transferred by physical means through wires (optical fibre, coaxial cables and twisted pair) or wirelessly (via satellites or cellular technologies)

Or based on the geographical area served, Networks are generally divided into WANs Wide area networks that span a wide geographical area such as a country or LANs, Local area network that span a building. In a geographical categorising of networks, two or more data transport media maybe used (wired or wirelessly).

4.2 Protocols

Protocols are a set of rules on how devices in a network should communicate with one another. To facilitate the smooth movement of data across different transportation medium protocols help to make sure that the data is addressed to the right recipient, it transmits the data through the network and receives the data on the receiving device. [23]

4.2.1 Protocol categories

Protocols can be categorised in terms of connection; they are either connection oriented where communicating devices exchange addressing information or connection less communication where devices do not send addressing information when sending data. Or most commonly protocols are categorised in

terms of layers; the most common models are OSI layer model and the TCP/IP layer model.

4.2.2 Protocol Layers

Encapsulation is used to group protocols in layers of general functionality The top layers are for application interactions and the lower layers are for the physical transmission, explained below is The TCP/IP layer model

Link Layer: The lowest layer in the TCP/IP model which can be used to connect networked hardware. It is responsible for tasks ranging from the preparation of data by adding packet information, transmitting the packets through a physical medium and converting device network addressing (IPv4/IPv6) to a data link addressing (MAC addresses). Common protocol is this layer is the ARP protocol. This layer corresponds to physical and data link layers in the OSI model.

Internet Layer: Contains protocols used for network routing, host addressing and identification through IPv4 a 32-bit system or IPv6 a128-bit system, this layer corresponds to layer 3(Network Layer) of the OSI model, a common protocol in this layer is, Internet Protocol: This protocol dictates how data is delivered across source and destination points in a best effort data delivery service. Data can be thrown away in case of network errors or data may not be delivered in the order it was sent. [17] [24]

Transport Layer: Implemented on top of the internet layer to add data reliability correspond to layer 4(also called transport layer) in the OSI model. Common protocols in this layer include:
User Datagram Protocol: works on top of the Internet protocol in a connection less set up where data is not sent with address information and works easily when the duplication and delivery of the data is not guaranteed. [18]
Transmission Control Protocol is an alternative to UDP. The transmission control protocol is a connection orientated protocol that can facilitate data transfer between two hosts by facilitating That connection that it initiates hence it is reliable and in control of data flow.

Application layer: The top most layer in the TCP/IP model containing protocols implemented on top of transport protocols to facilitate the exchange of data between applications across network connections A common protocol is the HTTP (hypertext transfer protocol). A protocol for text transfer and exchange between servers and browsers. It is built on top of the TCP protocol in the transport layer. The application layer corresponds to the session presentation and application layers in the OSI model. [24].

5 APPLICATION LAYER

The application layer can be further divided into two sub layers namely, a data management and an application service layer [10].

5.1 Data-management sub layer

The data management layer takes care of handling big data through cloud computing, intelligent classification of data and data mining.

5.1.1 Cloud Computing and Data Storage

Cloud computing is placing of services in a cloud so that users can access them anytime anywhere.

The services include storage, computational space, memory and applications therefore users do not need to directly install applications in their local environment They can log into a browser and use the applications in the cloud and get the desired output or users can store a large amount of data without having the infrastructure for it. A cloud is a central unit consisting of servers located in a specific geographical area that have larger storage spaces, processers and different applications that users can access and use without having to have these tools physically.

5.1.2 Data Mining

One of the main goals of IoT is the reduction of human input in the collection of data and analysis of data and this creates a window for Data Mining technologies. When very large amount of data is collected and stored in a database through perception by sensors, not all the data is of value to the end application/user, Thus, it is pre-processed to make it ready for mining through data cleaning, selection, integration and transformation Then intelligent computations are carried on the data to extract useful patterns or information. [20]

5.2 Application Service sub layer

After data has been processed and analysed, it is made available for different kinds of applications Some of the application areas include the following:

5.2.1 Smart Homes

In a home set up, home appliances for example doors, windows or fridge lights are embedded with actuators and different kinds of sensors. The appliances could be connected together by the ZigBee technology to form a home monitoring wireless sensor network that gathers data about the home and sends it to a data processing centre through Wi-Fi and 3G network technologies.

A User application will make use of the processed data to notify the user and to trigger action in the appliances through actuators by user input or automatically. For example, a window with a water sensor will dictate water and close itself in case of rain.

5.2.2 Smart Water

Sensors and actuators can be embedded in water supply pipes in a city. the embedded sensors are to detect defects in pipes or unnatural chemical composition of water and the embedded actuators are programed to react to the different readings of the sensors such as a cut of power supply and/or notify repairs service.

5.2.3 Smart Transportation

Is applied widely in traffic management to track speeding cars whereby Cameras with a speed sensing technology track the speed of cars passing by and in case of an over speeding car the system reacts by taking a number plate picture of the speeding car.

6 SECURITY IN THE DIFFERENT LAYERS

In an IoT set up security is always an issue because different ubiquitous devices connecting simultaneously and exchanging all kinds of data. To overcome this challenge the security in an IoT set up should be approached on a layer-by-layer basis as described In the following section. Different challenges on each layer are handled in more detail and the solutions from some researches are put forward [12].

6.1 Security of the Perception layer

The Security of the perception layer is a challenge since devices in this layer do not usually have enough memory and/or computational capacity for complete security technology. Thus attacks usually happen from external sources at the nodes where the collected data is passed on to the transport layer, for example where Wireless sensor networks connect to the Internet or external networks(gateways) [12]. Attacks in this layer are usually to disrupt object identification through disrupting of Mac addresses of devices and jamming of networks that connect sensor nodes. Hence data cannot be efficiently collected. [13] Security in this layer can be improved by applying Intrusion detection and Wireless encryption mechanisms. [12]

6.2 Security in Network Layer

The attacks from this layer can directly target the sensor and actuator nodes and alter their ability to collect and share data, alter the destination of information, alter actual record or information source, alter the information itself or block the connections between the perception layer and the application layer hence complete breakdown of the service. Some of the attacks in this layer include:

Flooding Originates from the network layer but targets the storage and processing capabilities of the devices in the perception layer, since the devices in this layer do not have much memory or computational capabilities it does not take much bandwidth to achieve flooding in a network of simple nodes.

Selective forwarding This is where an intermediary node only transmits selective data packets while blocking or dropping other packets.

Security can be improved by Access security to ensure that data and data routes are accessed by the authorized and authenticated entities, encryption of data as it is being transmitted and network intrusion detection systems should be put in place. [13][12]

6.3 Security in the application layer

As Data is being exchanged between different entities like databases and applications it is exposed to all kinds of attacks before it gets to the users of the information
Security threats can be from within the layer through mainly unauthorized access, theft of data, supply of fake data, worms and viruses. or the network layer through alter of data destination and source information [13] Access control management Privacy protection is used to improve security in the application layer. [12]

7 IOT APPLICATION EXAMPLES

IoT is applied in a number of industries today to achieve a wide range of goals and some of the application scenarios include the following:

7.1 Kemppi ARC system 3

Kemppi is a world leading manufacturer of arc welding equipment and a provider of welding solutions based in Lahti Finland. It has a welding management and documentation system that employs internet of things technologies called the Kemppi ARC system 3 or simply KAS3. (See figure 4 below)

It is set up in a way that Kemppi welding equipment have simple bar code readers, sensors and smart readers embedded to record the welding process. When smart readers sense beginning of a welding process data collecting starts, they record the welder ID through bar codes, take note of the equipment used in the welding process, the date and time of welding.

This information is then sent to a cloud service for the Automated data collection and management where data is compared to the planned work performance, specifications provided by customers it is also used to keep track of the welding equipment.

This leads to full monitoring of the welding network, traceability of the collected data and real time welding efficiency reports hence, the improvement of quality and productivity. [20]

FIGURE 4. Kemppi KAS3 set up [20]

7.2 Fara Technologies

Fara is a Scandinavian based company that provides solutions for cloud-ticketing and real time information systems for traffic and fleet management.

In Oulu Fara sophisticated information system is used to provide city dwellers with real time public transport updates. The Bus movement is tracked live and displayed on screens around bus stops so that passengers know where the bus is and its progress. (See figure 5 below).

Buses are fitted with sensors that send location updates every second to data centres which process the data and make it available to be displayed on the screens or the data is sent to traffic authorities, contractors and controllers. Drivers are also provided with tablets where they select the next destinations and can make a notification in case of delay. The Fara system also handles traffic priority for busses running late so that they can remain on schedule. Hence, the whole transport system is monitored and controlled [21].

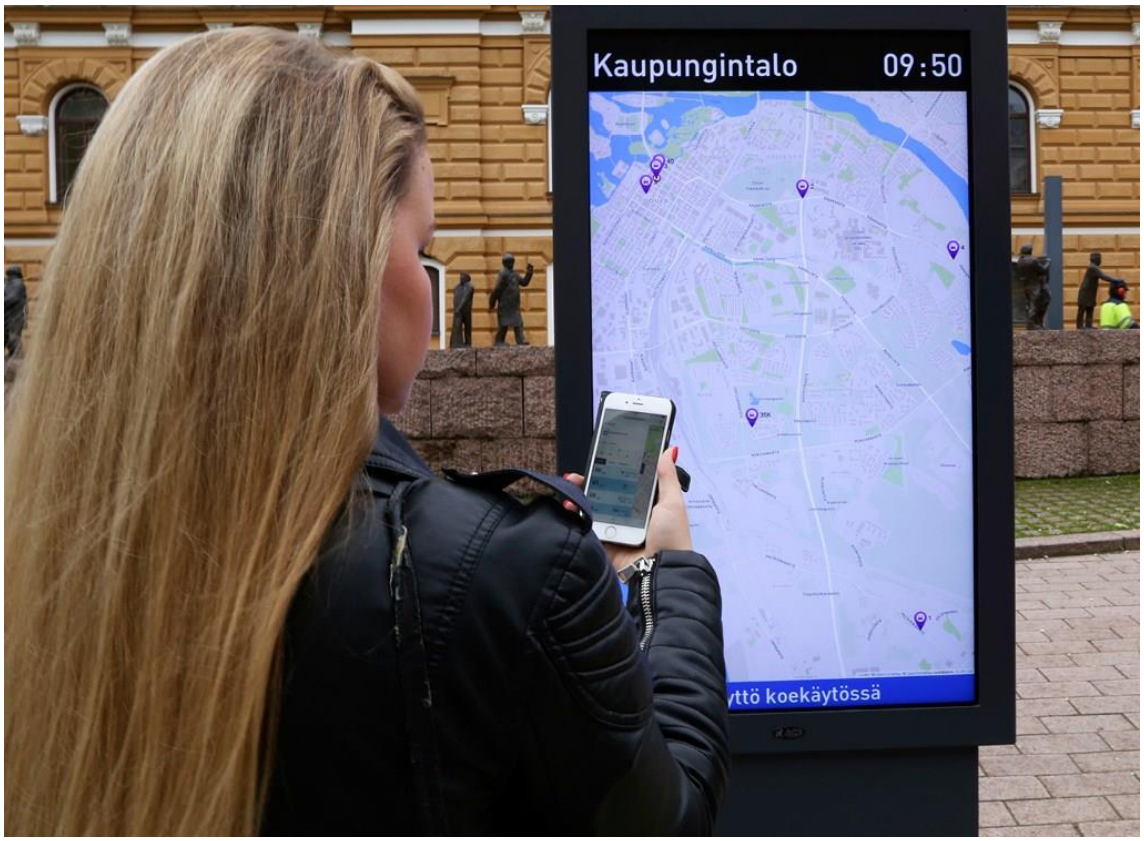

FIGURE 5. Image of one of the display screens in Oulu that displays bus location information in real time [21]

8 CONCLUSION

The Internet of Things is a diverse concept that involves interaction of diverse technologies. Therefore, there is no straight forward definition of what it is made of or what its key technologies are, Hence, there is room for more research to develop a standard architecture from which modifications can be made depending on the industry where it is applied.

Furthermore, for the Internet of Things to achieve full maturity human input must be eliminated in data gathering paving way for automated machines/devices that can independently collect data, send the data to processing centres where it is automatically processed and the devices can react according to the data collected. This would lead to the full automation of our daily lives and creation of artificially intelligent entities that we can interact with.

With the above conditions in place the potential application area will continue growing and it will range from environment monitoring and health sector to transport sector It is set to be a big business area and a new source of income for many IT companies and world governments.

Hence the result of the thesis is explanation and great understanding of internet of things root architectural structure and identification of some key technologies applied.

.

9 REFERENCES

1. Wu, M & Lu, T & Ling, F-Y & Sun, J & Du, H-Y. 2010. Research on the architecture of internet of things.
Advanced computer theory and engineering (ICATE) international conference 3 2010

2. Yun, M & Yuxin, B. 2010. Research on the architecture and key technology of IOT applied on smart grid.
Advances in energy engineering(ICAEE) international conference June 2010

3. Khan, R & Khan, S & Zaheer, R & Khan, S. 2012. Future internet: the internet of things architecture possible applications and key challenges.
Frontiers of information technology(FIT). 10th international conference Dec 2012.

4. Kevin, Ashton. That internet of things thing RFID journal. 1991.

5. Jun, Y & Yang, W. 2011. Internet of things: system framework, applications and attentions in program operation.
Computational problem-solving (ICCP) international conference, 21-23 Oct 2011.

6. Chong, G & Zhihao, L & Yifeng, Y. 2011. the research and implement of smart home system based on internet of things
Electronics, Communications and Control (ICEEC), International Conference. 2011.

7. Sehgal, K, V & Patrick, A & Rajpot, L, A. 2014. Comparative study of cyber physical cloud, cloud of sensors and internet of things: their ideology, similarities and differences.
Advanced computing conference (IACC) 2014 IEEE international,21-22 Feb 2014.

8. Jia, X & Feng, Q & Fan, T & Lei, Q. 2012. RFID technology and its applications in internet of things.
Consumer Electronics and networks (CECnet), 2012 2nd international conference 21-23 April 2012.

9. Chase, J. The Evolution of the internet of things. Texas Instruments. 2013.

10. LIU, J & Li, X & Chen, X & Zhen, Y & Zeng, L. 2011 Applications of internet of things on smart grid in china

Advanced communication technology (ICACT) 13th International conference. 2011.

11. Chen, D & Chang, G & Jin, L & Ren, X & Li, J & Li, F. 2011 A novel secure architecture for the internet of things.
Genetic and evolutionary computing 2011 fifth international conference. 2011

12. Pomponiu, V. 2014. Securing wireless ad hoc networks. State of the art and challenges. 2014. University of Tornio.

13. Chen, D & Chang, G & Jin, L & Ren, X & Li, J & Li, F, A. Novel secure Architecture for the internet of things. 2011
Genetic and Evolutionary Computing ICGEC September 2011.

14. Khalil, N & Mohamed, R & Benhaddou, D & Gerndt, M. 2014 Wireless sensors networks for internet of things.
IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing. 2014.

15. Gill, K & Yang, S-H & Yao, A. 2009. Zigbee home based automation system. Date of retrieval 5.10.2016.
http://ieeexplore.ieee.org.ezp.oamk.fi:2048/xpls/icp.jsp?arnumber=5174403.

16. Postel, J. 1981. Internet protocols Darpa Internet Program Protocol Specification. Date of retrial 9.10.2016.
https://tools.ietf.org/html/rfc791.

17. Postel, J. 1980. User Datagram Protocol. Date of retrieval 10.10.2016.
https://www.rfc-editor.org/rfc/pdfrfc/rfc768.txt.pdf.

18. Postel, J. 1980. Transmission control protocol Darpa Internet program protocol specification. Date of retrieval 11.10.2016.
https://tools.ietf.org/html/rfc793

19. Han, J & Pei, J & Kamber, M. 2012. Data Mining: Concepts and Techniques.

20. Kemppi, K. 2015. MI2015 Industry seminar. Date of retrieval 20.11.2016.
http://www.slideshare.net/Prizztech/io-t-in-welding/12

21. FARA. Cases Studies FARA. Date of retrieval 20.11.2016.
http://fara.no/en/company/case-studies/oulu-finland

22. FARA. 2014. FARA ASA Cloud ticketing and passenger services. Date of retrieval 20.11.2016. https://www.youtube.com/watch?v=hjunRZwTvaY

23. Mitchell, B. 2015. How Computer Networks Work- Protocols. Date of retrieval 20.11.2016. https://www.lifewire.com/computer-networks-protocols-817374

24. Wikipedia. Unknown. Internet protocol suite. Date of retrieval 20.11.2016. https://en.wikipedia.org/wiki/Internet_protocol_suite

25. Wikipedia. Unknown. IP address. Date of retrieval 20.11.2016. https://en.wikipedia.org/wiki/IP_address

26. Wikipedia. Unknown. Computer network. Date of retrieval 21.11.2016. https://en.wikipedia.org/wiki/Computer_network#Geographic_scale.