Volume 5 ▪ Issue 1 ▪ April 2013

Editor-in-Chief
Dr. Min Song

INTERNATIONAL JOURNAL OF COMPUTER NETWORKS (IJCN)

ISSN : 1985-4129

Publication Frequency: 6 Issues / Year

CSC PUBLISHERS
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF COMPUTER NETWORKS (IJCN)

VOLUME 5, ISSUE 1, 2013

EDITED BY
DR. NABEEL TAHIR

ISSN (Online): 1985-4129

International Journal of Computer Networks (IJCN) is published both in traditional paper form and in Internet. This journal is published at the website http://www.cscjournals.org, maintained by Computer Science Journals (CSC Journals), Malaysia.

IJCN Journal is a part of CSC Publishers
Computer Science Journals
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF COMPUTER NETWORKS (IJCN)

Book: Volume 5, Issue 1, April 2013
Publishing Date: 30-04-2013
ISSN (Online): 1985-4129

IJCN Journal is a part of CSC Publishers
http://www.cscjournals.org

Published in Malaysia

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers, 2013

EDITORIAL PREFACE

The International Journal of Computer Networks (IJCN) is an effective medium to interchange high quality theoretical and applied research in the field of computer networks from theoretical research to application development. This is the *First* Issue of Volume *Five* of IJCN. The Journal is published bi-monthly, with papers being peer reviewed to high international standards. IJCN emphasizes on efficient and effective image technologies, and provides a central for a deeper understanding in the discipline by encouraging the quantitative comparison and performance evaluation of the emerging components of computer networks. Some of the important topics are ad-hoc wireless networks, congestion and flow control, cooperative networks, delay tolerant networks, mobile satellite networks, multicast and broadcast networks, multimedia networks, network architectures and protocols etc.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Started with Volume 5, 2013, IJCN aims to appear with more focused issues. Besides normal publications, IJCN intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

IJCN give an opportunity to scientists, researchers, engineers and vendors to share the ideas, identify problems, investigate relevant issues, share common interests, explore new approaches, and initiate possible collaborative research and system development. This journal is helpful for the researchers and R&D engineers, scientists all those persons who are involve in computer networks in any shape.

Highly professional scholars give their efforts, valuable time, expertise and motivation to IJCN as Editorial board members. All submissions are evaluated by the International Editorial Board. The International Editorial Board ensures that significant developments in computer networks from around the world are reflected in the IJCN publications.

IJCN editors understand that how much it is important for authors and researchers to have their work published with a minimum delay after submission of their papers. They also strongly believe that the direct communication between the editors and authors are important for the welfare, quality and wellbeing of the journal and its readers. Therefore, all activities from paper submission to paper publication are controlled through electronic systems that include electronic submission, editorial panel and review system that ensures rapid decision with least delays in the publication processes.

To build its international reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCN. We would like to remind you that the success of our journal depends directly on the number of quality articles submitted for review. Accordingly, we would like to request your participation by submitting quality manuscripts for review and encouraging your colleagues to submit quality manuscripts for review. One of the great benefits we can provide to our prospective authors is the mentoring nature of our review process. IJCN provides authors with high quality, helpful reviews that are shaped to assist authors in improving their manuscripts.

Editorial Board Members
International Journal of Computer Networks (IJCN)

TABLE OF CONTENTS

Volume 5, Issue 1, April 2013

Pages

Towards Internet of Things: Survey and Future Vision

Omar Said *o.saeed@tu.edu.sa*
IT/ College of Computers and Information Technology
Taif University
Taif, Saudi Arabia.

Mehedi Masud *mmasud@tu.edu.sa*
CS/ College of Computers and Information Technology
Taif University
Taif, Saudi Arabia.

Abstract

Internet of things is a promising research due to its importance in many commerce, industry, and education applications. Recently, new applications and research challenges in numerous areas of Internet of things are fired. In this paper, we discuss the history of Internet of things, different proposed architectures of Internet of things, research challenges and open problems related to the Internet of things. We also introduce the concept of Internet of things database and discuss about the future vision of Internet of things. These are the manuscript preparation guidelines used as a standard template for all journal submissions. Author must follow these instructions while preparing/modifying these guidelines.

Keywords: Internet of Things, RFID, TCP/IP, Web Applications.

1. INTRODUCTION

Recently, the concept of the Internet as a set of connected computer devices is changed to a set of connected surrounding things of human’s living space, such as home appliances, machines, transportation, business storage, and goods etc. The number of things in the living space is larger than the number of world population. Research is going on how to make these things to communicate with each other like computer devices communicate through Internet. The communication among these things is referred as Internet of Things (IoT). Till now, there is no specific definition or standard architecture of IoT. Some researchers define the IoT as a new model that contains all of wireless communication technologies such as wireless sensor networks, mobile networks, and actuators. Each element of IoT is called a thing and should have a unique address. Things communicate using the Radio-Frequency Identification (RFID) technology and work in harmony to reach a common goal. In addition, the IoT should contain a strategy to determine its users and their privileges and restrictions. The US National Intelligence council has stated that by 2025 the IoT will connect everything in our life [1]. For this target new architectures are proposed and more research challenges are opened. Authors in [1] highlight some research challenges. Despite new architectures are proposed in the recent years, however, the future vision of IoT is still unclear. Considering the research challenges and future vision of IoT, in this paper we present a detail survey. At the end of the paper, we also present our recommendations.

The rest of the paper proceeds as follows. Section 2 demonstrates the history of IoT. Section 3 introduces the currently proposed IoT architectures. Section 4 introduces the IoT research challenges and open problems. Section 5 presents the IoT database. Section 6 discusses future vision of IoT. Section 7, demonstrates the comparison between our survey and other surveys. Finally, the paper concludes in Section 8.

2. THE IOT HISTORY

2.1 IoT Definition

Internet has become more prevalent in our lives in a shorter time period than any other technology in the history. It revolutionized the communicate way of people. Currently, the Internet involves the process of connecting machines, equipment, software, and things in our surroundings. This connection will be through the use of the unique Internet protocol address that permits things for communicating to each other without human intervention. This new scenario is called IoT [2]. The term IOT is formalized by MIT Auto-ID center at [3]. Till now there is no accepted or standard definition for IoT.

2.2 The IoT Applications

There can be many applications of IoT. The famous IoT application is in marketing. We know that a market contains many goods and electrical machines. By using IoT, an item can automatically contact its provider and inform its situation in case of stock decreasing [4]. The cooperation between the traffic lights and the sensors for environment pollution is another example that uses the IoT technology [1]. This cooperation using IoT may provide a life with new advantages such as the normal distribution of cars in the roads and the adaptive time for each sign to be on or off [5]. There is also a range of IoT applications in France. For example, the use of glass containers equipped with ultrasonic sensors that send information about its level of filling [1]. When the level reaches to three-quarters of the container, the collection, loading and unloading processes are started automatically. In the United States, there are many applications exist such as garbage cans that are provided with sensors. When the garbage reaches a certain weight or level, warning is sent to the municipality in order to send the garbage cars, which leads to reduce the taxes on homeowners and reduce the cost and the time of communication process [1]. Also, IoT and RFID technology are used to recycle information about automotives factories in china [6]. In addition, there are some projects, which are still under progress, e.g., e-learning, healthcare, smart environment (home, office, plant), and industrial fields [1, 7, 8].

Regarding the IoT and Internet applications, it is clear that the IoT applications and the Internet applications are similar. Based on the ontology, both applications have a common character. There are some close relations such as Hypertext and text, XML and electronic tag, and Standardization and free restrictions. The ascendancy of IoT comes from product information and Internet. The IoT is tangible restriction to the product information. The product information must be written on an electronic tag, with fixed format and standardized and general words. Internet of Things can be considered as a special application of Semantic Web. It tries to appreciate the mentally processing and sharing the product information based on the Semantic Web platform [9, 10].

3. THE IOT ARCHITECTURES

Recently, there are two IoT architectures are suggested (i) 3–layer architecture and (ii) 5-layer architecture, and other special purpose architectures, respectively [11, 12, 13, 14]. In the following, we present these architectures.

3.1 The 3-Layer architecture

Beginning of the IoT, the accepted architecture was the 3-layer architecture. It consists of three layers which are called perception, network, and application. The purpose of perception layer is to identify each thing in the IoT system. This is done by gathering information about each object. This layer contains RFID tags, sensors, cameras, etc. The second layer is the network layer. The network layer is the core of the IoT. It transmits the information gathered by the perception layer. It contains the software and hardware instrumentations of internet network in addition to the management and information centers. The third layer is the application layer. The application layer's target is to converge between the IoT social needs and industrial technology (i.e. it can be considered as the middle tier between the industry technologies and how it can be controlled to cover the human needs) [11], see Fig. 1.

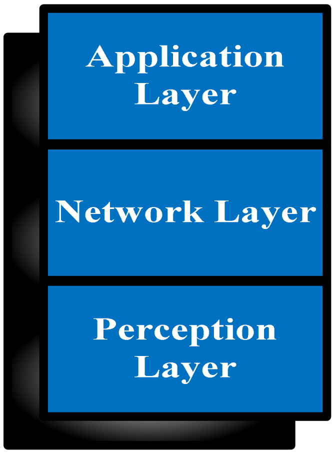

FIGURE 1: The IoT 3-Layer Architecture [11].

3.2 The 5-Layer Architecture

The 3-layer architecture became not sufficient due to the expected IoT development. Therefore, 5-layer architecture is proposed. The first layer is called business. The purpose of this layer is to define the IOT applications charge and management. Also, it is responsible about the user's privacy and all research related to IOT applications. The second layer is called application. The target of this layer is determining the types of applications, which will be used in the IoT. Also, it develops the IOT applications to be more intelligence, authenticated, and safe. The third layer is called processing. Its responsibility is to handle the information gathered by perception layer. The handling process contains two main topics; storing and analyzing. The target of this layer is extremely hard due to the huge gathered information about system things. So, it uses some techniques such as database software, cloud computing, ubiquitous computing, and intelligent processing in information processing and storing. The fourth layer is called transport. It seems like the network layer in the 3-layer architecture. It transmits and receives the information from the perception layer to the processing layer and via versa. It contains many technologies such as infrared, Wi-Fi, and Bluetooth. Also, the target of this layer is to address each thing in the system using IPV6. The fifth layer is called perception. The target of this layer is to define the physical meaning of each thing in the IoT system such as locations and temperatures. It also gathers the information about each object in the system and transforms this data to signals. In addition, it contains the technologies that are used in the IoT such as the RFID and the GPRS [11]. Fig. 2 presents the 5-Layer architecture.

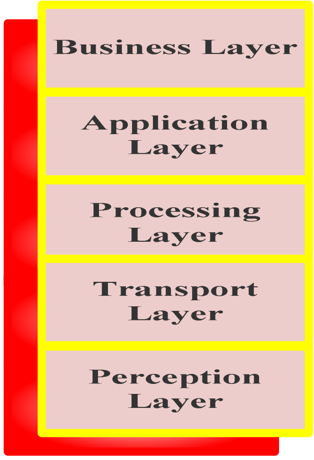

FIGURE 2: The IoT 5-Layer Architecture [11].

3.3 Special Purpose Architectures

There are some special purpose IoT architectures. The first architecture [15] is related to media-aware traffic security architecture. This architecture is based on the given traffic classification to enable various multimedia services being available anywhere and anytime. The second architecture [16] is new clock synchronization architecture of network for IoT. This clock synchronization architecture of IoT is the key technology to resolve the problems, which are released due to manage the IoT nodes effectively and to ensure high clock synchronization precision. It includes three levels: adaptation level, organization level and region level. The adaptation level architecture is to resolve the problem about the adaptability of IoT; the organization level architecture is to organize and manage of the clock synchronization system; the region level architecture is to ensure clock synchronization accuracy and security. The third architecture [17] is for trusted security systems. This architecture is based on cholars' researches and combined with the security requirements and characteristics of IoT. This architecture also includes trusted safety management system, security gateway, unified service platforms of IoT, security infrastructure, and unified information exchange platform. The fourth architecture [18] is mankind neural system. This architecture introduces two aspects: Unit IoT and Ubiquitous IoT. The Unite IoT focus on special targets (provides solutions for special applications), and its infrastructure is a man-like nervous system. The Ubiquitous IoT focus on the collection of multiple unites of IoTs with ubiquitous views (assemble the special organization to be manageable by one powerful application). Also, there are some special purpose architectures [19, 20, 21] which cannot be considered a standard architecture.

4. IOT CHALLENGES AND OPEN PROBLEMS

There are numerous challenges in the IoT which are still under research. The IoT challenges and open problems are raised due to two main reasons. These reasons for mass gathering information for each thing in the IoT system and the communication among system hardware, see Fig. 3.

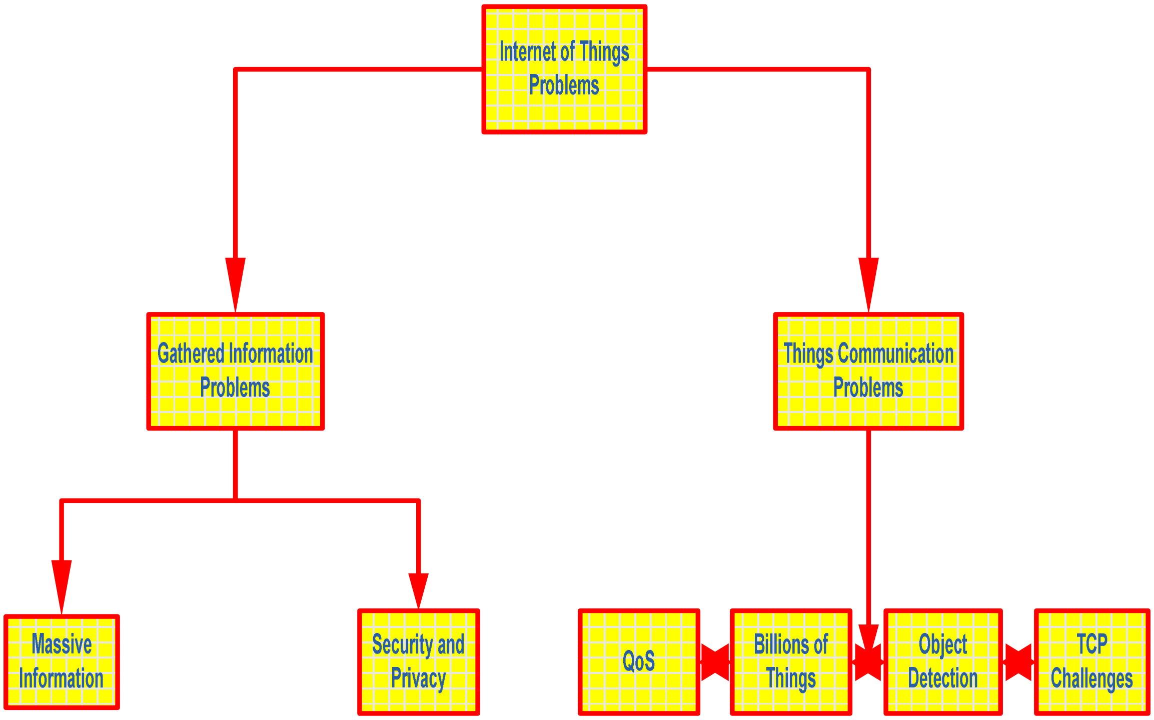

FIGURE 3: IoT Challenges and Problems.

4.1 Information Gathering Problems

These problems can be divided to two main classes. The first one is related to the massive information that is gathered by RFID about huge number of things which are found at IoT system. The second is the security and the privacy of information due to wireless transmission media.

Massive gathered information: The IoT systems should have millions if not billions of objects. Each object should radiate information to express about itself. This information should be gathered. The quantity of gathered information is massive due to the huge number of IoT objects. So, there are several problems which are raised due to a lot of gathered information. These problems are transmission, storing, and processing. Transmission problem means that it is required to transmit all of things data in real time and this is not a guaranteed issue [22, 23]. This is because of the bandwidth issue, which is required to transmit this information, may be not available. It is well known that the information travels in a trip starting from the things and ends to its control web application. This trip may contain more bandwidth bottlenecks which mean that a required bandwidth is mostly not available. The problem of data storing is raised due to the quantity of media required to store and backup this information. The processing operation means that the things information should be handled by IoT web applications to determine the control actions for each thing. This handling process should be done in a real time mode [24, 25].

Security and privacy: It's well known that the data is transmitted between IoT objects inside a wireless medium. So, the security and privacy issues are very important and should be discussed. Regarding the security problem, there are numerous causes to make the IoT information in danger. These causes are physical attack, wireless information attack, and low self-defense. The physical attack means that the hacker may tamper with the IoT devices due to presence of these devices alone most of the time. Hence, anyone can hack it physically. The wireless information attack means that the hacker can acquire the information from the medium before it is received by the destination and there are more researches in this topic [26, 27, 28, 29]. The low self defense means that most of IoT devices didn't have an ability to accept security package(s) for partially saving [30, 31, 32].

The privacy is an important issue in civilized countries. It means that the information provider is only able to infer by observing the use of the system related to each system client (at least, inference should be very hard to conduct). The data collection, handling, and mining are accomplished in the IoT systems in completely different form that we know. This is because there are more situations that may occur in the IoT system such as home resources control system. So, to guarantee the privacy of things personal information, we should make sure of three main items; (1) who collects the personal data, (2) how these data are collected, and (3) the time of collection process. Furthermore, the personal data that are collected should be used by authorized the person, stored in an authorized server, and accessed by authorized clients [33, 34, 35].

The security and privacy needs three main requirements: resilience to attack, data authentication, and client privacy. Also, some questions related to human rights and constitutional framework are raised such as if new international laws are needed, if legislation is envisaged [1, 36].

4.2 Things Communication Problems

The problem related to the communication between IoT things components, is divided into two classes. The first is addressing of things problem and the second is RFID problems in reading, writing, and transmission of objects information. In the following, we discuss the things communication problems.

Billions of IoT things: When we think in communication process among a large number of things, we observe a big problem due to many issues. Sample of these issues are: what is the hardware, which is required for communicating this massive number of things? What is the ideal addressing technique (protocol) for each thing in the resulted system? If the answer is IPV6, another question will be raised; if IPV6 is suitable for the IoT future? The compatibility between a huge number of required hardware, which consist the IoT systems, can be considered as a communication factor or not? and others. There are many attempts that have emerged to answer these issues [37, 38, 39, 40, 41, 42, 43], but most of these researches are theoretical and lack in practice. Furthermore, they did not specify the IoT future vision and parameters. The problem of the tools, which are proposed so far to build an integrated IoT system, is incomplete and lacking in standard. Another trial for accessing the information instead of using hardware communications (RFID) is presented in [44]. This trail uses the computer vision and image processing techniques to access the thing information and suffers from delay due to the time consumption in object image handling process (see subsection entitled real time object detection).

IoT and TCP challenge: The IoT infrastructure is similar to the Internet backbone. So, the data transmission will use TCP or UDP protocols as a transmission protocol. The UDP is not reliable protocol and this is opposite of our target. Hence, TCP should be selected to act as a transport layer for IoT systems. The TCP has more challenges related to the IoT systems such as connection setup, congestion control, and data buffering. The connection setup may not be considered in most cases in the IoT systems due to the need to transmit small amount of data between objects. In addition, the communication resources in IoT are mostly sensors, RFID tags, and PDAs which cannot handle the data required for connection setup. The congestion control is a challenge in the wireless medium which is the same medium of IoT systems. Also, in case of small transmitted information between IoT objects, the congestion control data is not required. The data buffering in TCP is required at the source for retransmission process and destination for ordering process. The data buffering processes are costly for the battery-less devices such as RFID tags. So, the conclusion is UDP is not suitable and TCP has more challenges and in most IoT cases is not required. Many researchers studied the characteristics and actions of transmitted information inside IoT objects such as WSN and RFID systems [22, 23, 24].

Real time objects detection: When we concentrate in IoT system, we find two ambiguous queries; how we can define each thing and how we can acquire its information. It is natural if we answer by using the RFID, the EPC, or the UID technologies. But, these technologies have several problems such as radiation, privacy, violation, and inconvenience of information updating. In addition, it is not easy to define all of these technologies with the entire world things shortly. There are many researches tried to solve these problems such as [45], [46]. Authors in [44] introduce another idea which changes the concept of using above technologies for things definition. Instead of using the RFID, the EPC, or the UID, we can use the computer vision and image processing techniques such that each object can extract other objects by vision. Also, this idea faces another challenge, namely the real time handling. The real time handling means that the relation between the IoT system objects, which contains three main steps; seeing, analysis, and information extraction should be accomplished in real time mode.

IoT QoS: There are many researches in the internet QoS such as [47, 48]. But these scenarios are not suitable for the IoT systems. This is because the QoS researches considered a localized area in the IoT such as Wireless Sensor Network (WSN) and not for other areas such as the RFID. The research of QoS may be applied on the IoT systems but this can be considered as a short term solution. In addition, the QoS results are executed on the M2M communication. But, in case of IoT, there are different paradigms due to the mixture of IoT objects each one has a different characteristics and behavior [1, 2].

4.3 Core Challenge

The most important factor in the IoT is to build a standard and universal architecture. So, now we try to construct this architecture based on our daily live. The attempt, which is introduced in [18], is much closed idea to our trial. This attempt is limited. The limitation of this architecture comes from the consideration that the entire IoT systems have the same features and layers. This is not true in most cases. In IoT infrastructure, there are many systems with different targets, applications, and features. Hence, we should expand the architecture, which is introduced in [18], to be the most common one that will communicate these different systems (work in this architecture in progress).

5. IOT DATABASE

Internet of Things system produces mass information. The format of RFID contains three parts EPC which represents the unique identifier read by an RFID reader; location is the place where the reader is found, and time of reading process. It is well known that RFID raw needs approximately 18 bytes. If we took a supermarket as an example, there are about 700,000 RFID tags. If the supermarket has readers that scan the items every second, about 12.6 GB RFID data will be produced per second, and the data will reach 544TB per day. So, it is necessary to find effective methods for storing, filtering and modifying RFID raw data. The Internet of Things gathered information can be classified into numerous types: RFID data stream, address/unique identifiers, descriptive data, positional data, environment data and sensor network data etc. [49]. It is a great challenge to manage the Internet of Things information. Many trials have appeared to suggest models for dealing with this type of intensive database. Reference [50] provides a new model called ROAM and used for variance detection in moving objects. Reference [51] developed a novel partition-and-detect model for faraway trajectory detection of moving object. Reference [52] also put forward a new method called TraClass using trajectory-based clustering and hierarchical region-based. Reference [53] introduced a new model in trajectory clustering of moving object which is called a partition-and-group. Reference [54] proposed a general model to supervise learning under the conditions of power, computational, and memory limitations. The special characteristics of IoT such as mass data, distributed data, time-related data, and heterogeneous environment bring several problems to centralized data mining architecture [55]. The last trial [56] suggested four different models. The first model, called multi-layer data mining model for IoT, which consists of four layers each one accomplishes some functions. These layers are data management layer, event processing layer, data mining service layer, and data collection layer, and each layer has many functions. The second model is called distributed data mining model for IoT. In this model, there is a core for entire data mining system which is called the global control node. It determines the data mining algorithm and the data sets for mining, and then search about the sub-nodes containing these data sets. Hence, these sub-nodes receive the raw data from various smart things. These information is filtered, abstracted, and compressed, and then is saved in the local data warehouse. The third model is called grid based data mining model for IoT. IoT objects should intelligent, context-awareness, and long-range operable. Therefore smart IoT objects are considered as a kind of resources for grid computing. Thus, using the data mining services of grid to implement the data mining operations for IoT is the core of this model idea. The fourth model is called data mining model for IoT from multi-technology integration perspective. In this model, the context-awareness provides the IoT system with data individually or from smart objects. IPV6 protocol is used in objects addressing. There are different ubiquitous ways are used for accessing the future Internet such as, sensor devices, RFID, WiMAX, etc. Credibility and controllability of data transmission are adapted by a trusted control plane. So, data mining tools and algorithms are carried out, and different service-oriented applications such as intelligent transportation, intelligent logistics accepts the gained knowledge.

5.1 Suggested IoT Database Architecture

We propose a multilayer data mining model for the proposed system based on [56]. The model consists of six layers: IoT layer, data collection layer, data warehousing layer, event processing layer, data mining service layer, and application layer. Table 1 describes each layer's functions while Fig. 4 presents a general view of the data model. Table 1demonstrates Functions of the Data Model Layers.

Layer Name	Layer Function
IoT layer	This layer contains all the system objects such as sensors, PDA, desktops, cameras, actuators, etc. In this layer each object is identified using RFID and IPv6.
Data collection layer	This layer collects the objects' data. Each type of data needs different collection strategies such as misreading, repeated reading, fault tolerance, data filtering and communications, etc. This is a challenging task and should be solved appropriately.
Data warehousing layer	The collected data is stored in a data warehouse after three processes: object identification, data abstraction and compression. For example, the style of an RFID stream is "Electronic Product Code (EPC), location, time", where EPC marks smart object's ID. After data cleaning, we can obtain a Stay table that contains records of the format "EPC, location, time_in, time_out". We can, then, use a data warehouse like RFID-CUBOID to save and manage the data, including tables such as Info table, Stay table and Map table. Based on RFID-CUBOID, users can access online RFID data conveniently. Also, it may contain some XML modules that can be adopted to describe data in IoT. The connection between IoT smart objects are mostly achieved via the data warehousing layer in the IoT.
Event processing layer	Event processing layer is used to analyze events in IoT effectively. The data should be aggregated, organized and analyzed according to events. Hence, we can issue an event-based query or conduct an event-analysis in this layer. To that end, we should filter out primitive events so only complex events that concern user(s) are kept.
Data mining service layer	The data mining layer relies on both the data warehousing layer and the event processing layer. Object-based or event-based data mining services, such as association analysis, patterns mining data classification, data forecasting, data clustering, or outlier detection are available for applications. The architecture of this layer is service-oriented.
Application layer	The application layer contains three sub-layers: the local manager sub-layer, general manager sub-layer, and inelegant applications sub-layer. The fist sub-layer is used to implement some data mining algorithms for complex events that cannot be done in the data mining layer. The second sub-layer is used to aggregate, adapt, and filter the results that come from the local managers. The results are transformed to instructions and then into actions to be executed by the application sub-layer.
Multi-Agent system	Layers 2 to 6 are controlled by the multi-agent system.

TABLE 1: Functions of the Data Model Layers.

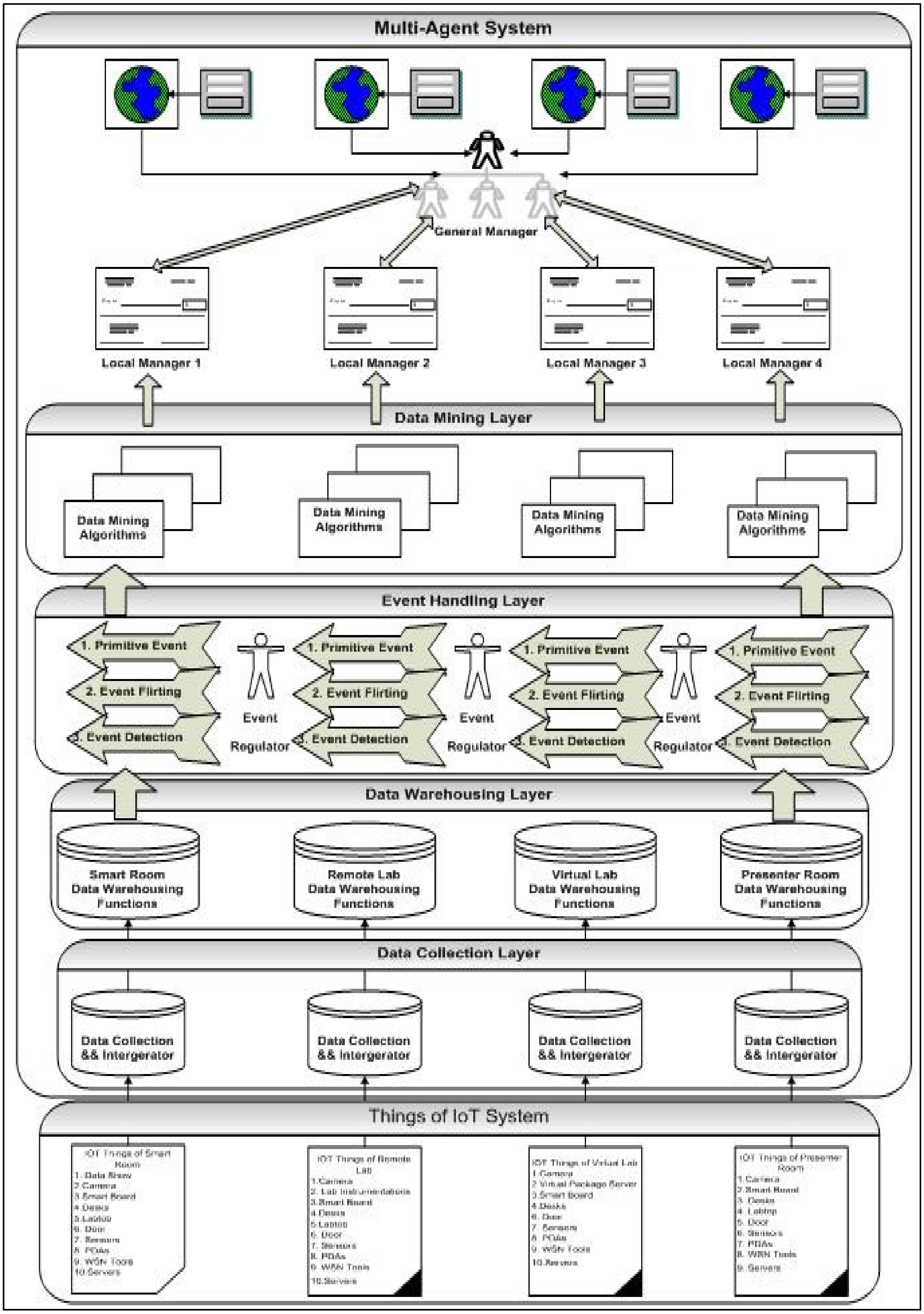

FIGURE 4: General View of the Data Model.

6. IOT DISCUSSION AND FUTURE VISION

In this section we discuss some issues regarding the IoT. Before we demonstrate our vision in IoT we first give an example: Consider a scenario where a person lives in a smart city. When the person wakes up from sleep, there is a set of events occurs between his waking up until he returns to his home (i.e. work hours events). First, he goes to the bathroom. The bathroom door is automatically opened. Then the faucet water is opened for adaptive interval time. As this person comes in the front of the apartment door, it is opened. While the person moves to the elevator, its door will be opened and the elevator is adapted to stop at the person desired level. These smart actions from the things that will be used by this person will continue until he reaches his work. If he wants to know information about something within the trip, he can easily access it by other things which are closed to the target one. This scenario is accomplished by communicating the system things (bathroom door, faucet water, apartment door, elevator, etc.) to be one network using IoT technology (smart application). This network makes the objects behavior like a human.

From above example, it's clear that our future vision of IoT is to make everything like an autonomous robot. This is a truth, which should be reached, but nowadays, this is not easy to accomplish. Science, there are more things which are passive. In addition, to transform each thing in our live, even it is active, from human control to full smartness is extremely expensive [57, 58]. Without complexity, the full smartness of a thing can be defined as the ability to make this thing behavior like a human behavior using software and hardware. Let us take a thing such as smart board and imagine that we would like to transform it into full smartness. The smart board can be considered as an active thing. This smart board should sense a human (student or professor) desires in addition to its around hardware tools such as data show and cameras. To accomplish these two simple characteristics, we need camera, image processing technique, processor, actuator, and intelligent program to adapt the smart board motion. All of these components are needed for transforming the active thing from static situation (i.e., with human controlled) to smartness.

From our point of view, in the near future we will find that most of these things in our range of living will be smart. In this case, we will find ourselves facing an amazing programming challenge to achieve the ultimate goal of IoT, see Fig. 5.

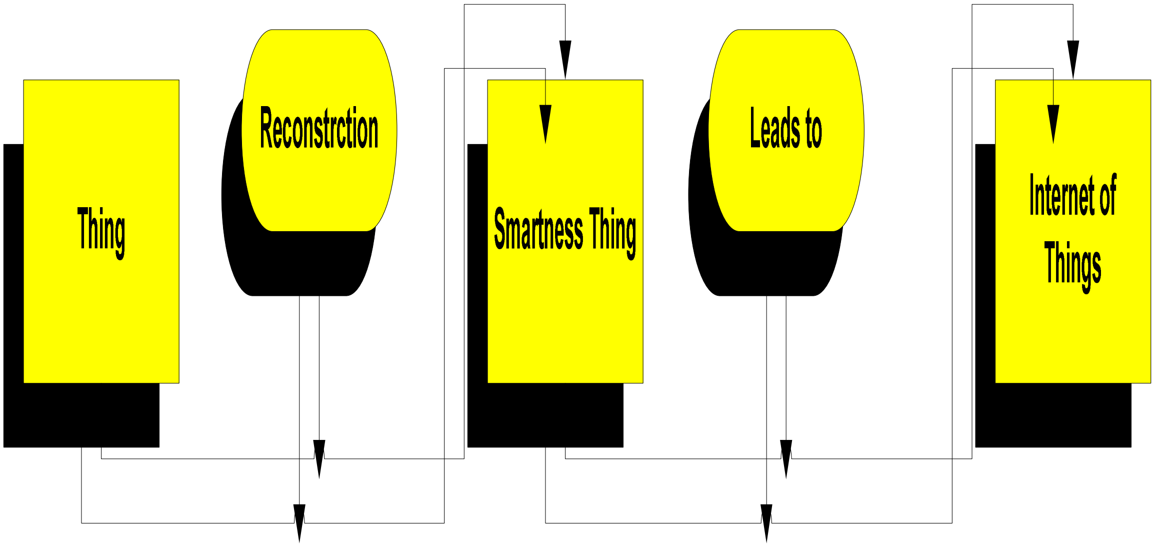

FIGURE 5: Live Cycle of Thing To Be in The IoT System.

If everything is transformed to smartness another problem will be raised that is called standardization. The standardization in the IoT system means the capability of replacing or changing hardware with something else; permitting mutual substitution without loss of function or suitability. The standardization itself may be a good solution for most of IoT problems if it is accomplished for most of the world things. It is well known that there are many systems in the IoT. Each IoT system is constructed using some hardware and software programs. The hardware in each system may be adapted in some way which cannot be used by other systems. For example, the marketing is a famous application in the IoT. The refrigerator is one of essential components in the market. The IoT refrigerator is adapted to call the service provider automatically in case of near to finish. If we use this refrigerator to be in a hospital, there are two different parameters. The first parameter is to whom the alarm message will be sent from the hospital refrigerator (i.e., there are more persons should be alarmed with the refrigerator situation) and the second one is the content sensitivity (the refrigerator should contain cadavers). Also, the IoT software may differ from one application to others. So, our recommendation is to strive for setting a standard specs for IoT hardware and software to be ready to work when transferred from one place to another. This thing will lead us to reduce the complexity of IoT and solves more problems such as compatibility, cost, and communication complexity, see Fig. 6.

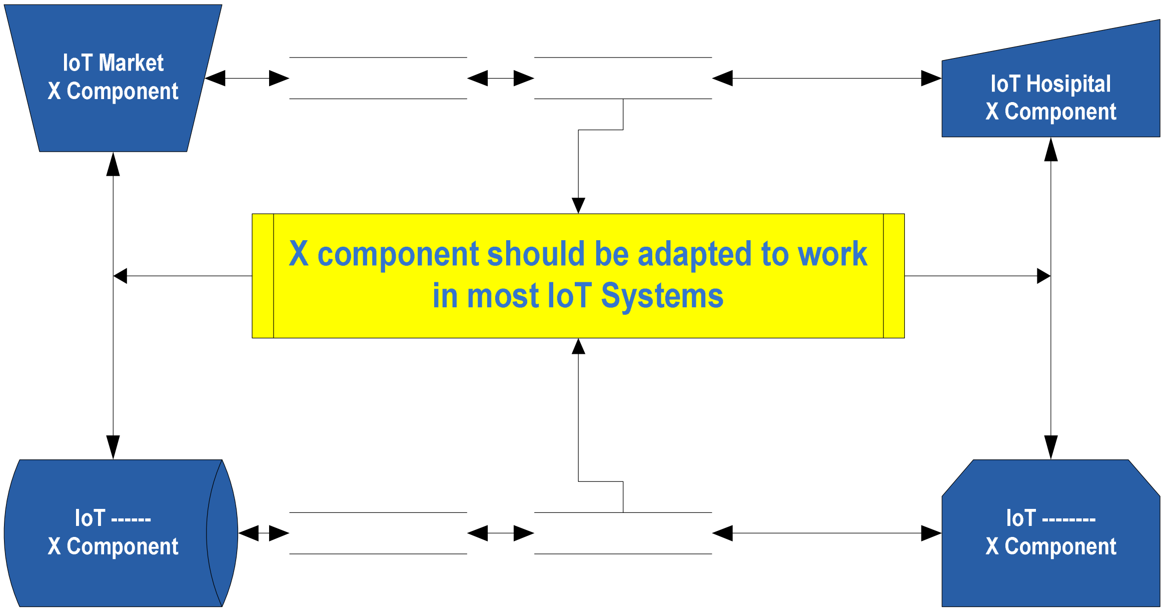

FIGURE 6: Standardization of Things In The IoT Systems.

Regarding the mass gathered information, I think we should determine the information, which is strictly useful for IoT and should be gathered. This determination will decrease the size of gathered information, hence the time that should be taken in gathering, transmission, processing, and filtering processes will be decreased. The standardization may participate to reach this target. If the hardware and the software characteristics for IoT systems are settled, only the information, which will be useful systems, is determined and accessed. The determination process may be accomplished using some techniques such as back propagation or feedback. When we install many IoT applications, the data of each system component, which is used in control mechanism, should be filtered and minimized. The filtering process will continue till the fully useful data is exactly determined. When the data of each component will be preciously known, the data can be stored on one server and accessed for the same components found all over the world. At this moment the number of gigabytes required for storing the IoT system information and the time required for process are minimized, see Fig. 7.

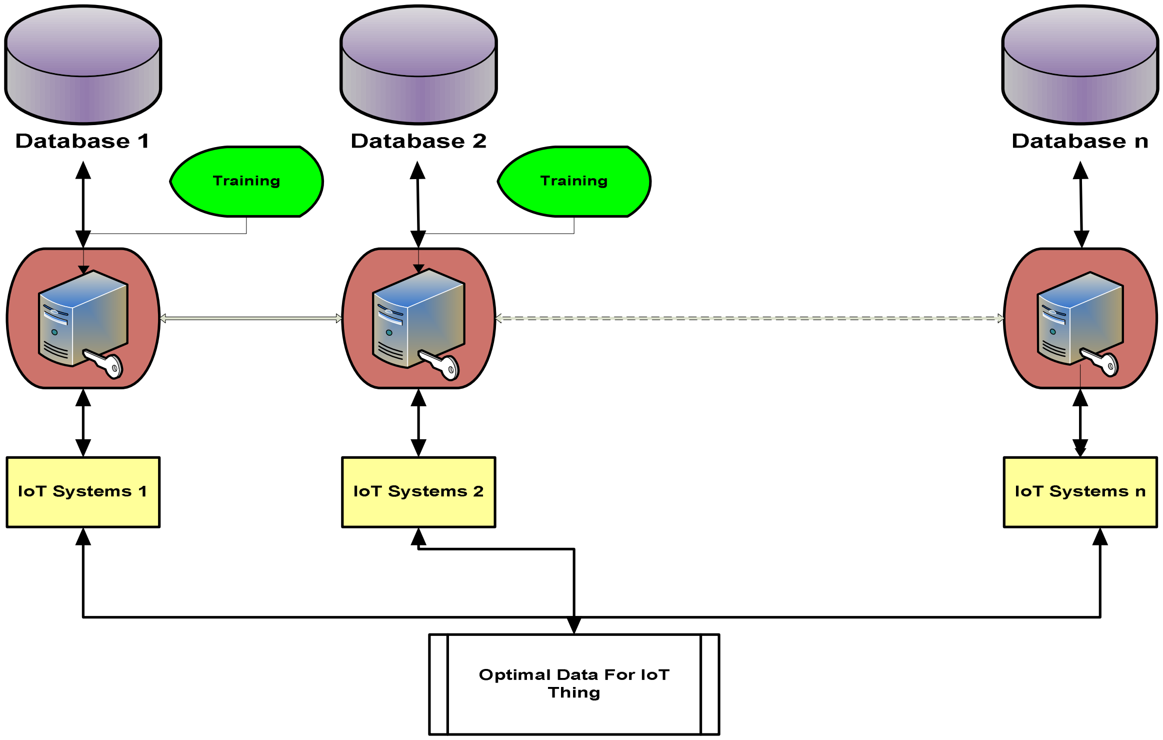

FIGURE 7: Accurate Information About Each IoT Thing.

Also, it's notable that the main problems are raised from the s character which is found in the things word. So, if we change our vision of IoT as a number of terrible things in a single network to little number of networks connected by one network, the problems may calm down. The division of the IoT system into IoT subsystems provides the researchers with more concentration in building an optimal infrastructure of IoT systems, see Fig. 8. For example, we consider the healthcare, the transportation and the marketing are three standalone IoT applications. In fact, we should change our vision and consider these applications as one application and is divided into three sub applications. This will lead us to delete the things duplication. The things duplication may be raised from the shared things in each IoT application. These shared things such as shelves, tickets, camera, desks, etc. it is sufficient to store the minimal control data about the thing one time instead of more times. In addition, we should construct a relation between the IoT subsystems. These relations help us in solving many of IoT challenges like things addressing.

The acronyms M2M stands for machine to machine communication. This abbreviation means that each machine can connect and construct a dialog with other machines. This expression is not new but it strongly appears with the IoT technology. Our vision in this issue is transforming the M2M communication to Data-to-Data (D2D) communication. Really, the IoT technology relies on the communication between the system machines and makes them in cooperation without human intervention, but this cooperation depends on the information, which is exchanged between devices, and the management information, which is used by the control web applications. Hence, the communication and control infrastructures are accomplished basically by the data. This concept fires the acronyms D2D instead of M2M., see Fig. 8.

The addressing problem is raised due to the massive number of things in IoT system. As stated above that the IPV4 and IPV6 may be used in addressing. The IPV4's main problem is addressing limitation. The problems in IPV6 are the security, routing, and mobility. There are more trials are found to solve the compatibility between the IPV6 backbone to be adapted with the IoT infrastructure specially in addressing of RFID tags. Recently, mixing of RFID tags into

IPv6 networks has been researched and techniques to add RFID identifiers and IPv6 addresses have been demonstrated in [59]. For example, the 64 bits are used to address the gateway between the internet and RFID system, and the other 64 bits are used to as an identifier of the IPv6 address to report the RFID tag identifier [60]. This trial cannot be used in case of 96 bits RFID identifier as found at EPCglobal. This problem is solved by deploying an agent to maps the RFID identifier into 64 bits to be used as an ID of IPV6 address. This mapping should be kept by this agent [61]. Another trial is introduced in [RFID URL]. This trial illustrates that IPV6 packet contains the body and the header of RFID message. There is another important issue regarding IPV6 and IoT addressing that is called mobility. We still in need to a technique describe the mobility issue in the IoT systems with guarantee of scalability and reliability with IoT heterogeneous environment. Also, How to obtain the IoT system addresses is an important issue should be adapted. In the IoT, the Object Name Service (ONS) should be able to combine the RFID tag identifier with the explanation of its object, and vice versa. The reversion process requires special techniques such as Object Code Mapping Service (OCMS) [62, 63].

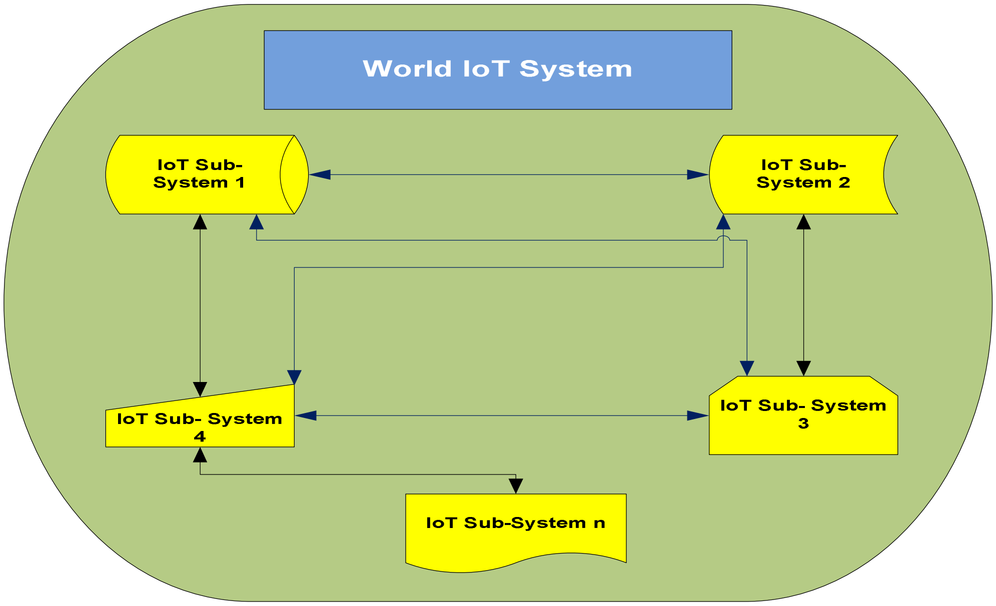

FIGURE 8: The IoT Should Be One System Contains Number of Related Sub-Systems.

7. OUR SURVEY vs. OTHER SURVEYS

The difference between our survey and other surveys [1], [23] is demonstrated below in Table 2. There are many parameters which are discussed in our survey and neglected in others such as IoT database and IoT core challenges. Also, there are some parameters which are extremely discussed in our survey and briefly discussed in others like IoT architectures.

Criteria	Our Survey	First Survey [1]	Second Survey [23]
IoT Application	Briefly Discussed	Extremely Described	Extremely Described
IoT Architecture	Extremely Discussed	Not Found	Not Found
IoT Database	Discussed	Not Found	Not Found
IoT Challenges	Discussed	Described	Extremely Described
IoT Future Vision	Extremely Discussed	Not Found	Briefly Discussed
IoT Open Issues	Described	Described	Not Found

TABLE 2: The Comparison Between IoT Surveys.

8. CONCLUSION

In this paper, an IoT survey is presented. IoT history, which contains the IoT definition and the applications, are demonstrated. Also, the IoT architectures, which are called 3-layer and 5-layer, with recent special purpose ones are showed. The IoT challenges such as the mass gathered information, security, privacy, and some networking challenges are introduced. In addition, the IoT database requirements, trials, and models are demonstrated. Finally, our IoT future vision is discussed.

9. REFERENCES

1. Luigi A., Antonio I., Giacomo M. 2010.The Internet of Things: A survey. Science Direct journal of Computer Networks, Volume 54, Pages: 2787–2805.

2. Yinghui H., Guanyu L., 2010. Descriptive Models for Internet of Things. IEEE International Conference on Intelligent Control and Information Processing, Dalian, China, Pages: 483-486.

3. Mealling M, 2003 Auto-ID Object Name Service (ONS) v1.0, Auto-ID Center Working Draft.

4. Bo Y., Guangwen H., 2008. Application of RFID and Internet of Things in Monitoring and Anti-counterfeiting for Products. International Seminar on Business and Information, Wuhan, Hubei, China, Pages: 392- 395.

5. Zouganeli E., Einar Svinnset I., 2009. Connected Objects and the Internet of Things - a Paradigm Shift. International Conference on Photonics in Switching, Pisa, Italy, Pages: 1-4.

6. Tongzhu Z., Xueping W., Jiangwei C., Xianghai L., Pengfei C., 2010 .Automotive recycling information management based on the internet of things and RFID technology. IEEE International Conference on Advanced Management Science (ICAMS), Changchun, China, page(s): 620 – 622.

7. Muriel D., Juan F., 2010. Expanding the learning environment: combining physicality and virtuality The Internet of Things for eLearning. IEEE International Conference on Advanced Learning Technologies (ICALT), Sousse, Tunisia, Pages: 730- 731.

8. Gustavo G, Mario O., Carlos K., 2008. Early infrastructure of an Internet of Things in Spaces for Learning. Eighth IEEE International Conference on Advanced Learning Technologies, Cantabria, Spain, Pages: 381-383.

9. Yinghui H., Guanyu L., 2010. A Semantic Analysis for Internet of Things. IEEE International Conference on Intelligent Computation Technology and Automation, Shenzhen, China, Pages: 336- 339.

10. Yuxi Liu, Guohui Zhou, Key Technologies and Applications of Internet of Things, IEEE Fifth International Conference on Intelligent Computation Technology and Automation, Hunan China, pp: 197-200, 2012.

11. Miao W., Ting L., Fei L., ling S., Hui D., 2010.Research on the architecture of Internet of things. IEEE International Conference on Advanced Computer Theory and Engineering (ICACTE), Sichuan province, China, Pages: 484-487.

12. Jinxin Z., Mangui L., 2010. A New Architecture for Converged Internet of Things. International Conference on Internet Technology and Applications, Beijing, China, Pages: 1 - 4.

13. Zhang J, Liang M., 2010. A New Architecture for Converged Internet of Things. IEEE International Conference on Internet Technology and Applications, Wuhan, China, Pages: 1-4.

14. Inge G., 2008. Architecture for the Internet of Things (IoT): API and interconnect. 2nd

International Conference on Sensor Technologies and Applications, Cap Esterel, France, Pages: 802-807.

15. Liang Z., Han-Chieh Chao, Multimedia Traffic Security Architecture for the Internet of Things, IEEE Networks, 2011. VOL.25, NO. 3, Pages: 35-40.
16. Junwei Lv, 11, Xiaohu Yuan and Haiyan Li, 2011. A New Clock Synchronization Architecture of Network for Internet of Things, International Conference on Information Science and Technology March 26-28, 2011 Nanjing, .Jiangsu, China, Pages: 685-688.
17. Xiong Li, Zhou Xuan,Liu Wen, 2011. Research on the Architecture of Trusted Security System Based on the Internet of Things, Fourth International Conference on Intelligent Computation Technology and Automation, Shenzhen, China, Pages: 1172-1175.
18. Huansheng N., Ziou Wang, 2011. Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework?, IEEE COMMUNICATIONS LETTERS, VOL. 15, NO. 4, Pages: 461
19. Castellani, et. al., 2010. Architecture and Protocols for the Internet of Things: A Case Study, IEEE Pervasive Computing and Communication Workshops (PERCOM Workshop), Mannheim, Germany, Pages: 678-683
20. Castro, M. et. al., 2011. Oxygen Cylinders Management Architecture Based on Internet of Things, International Conference on computational science and its applications (ICCSA), Murica, Spain, Pages: 271-274.
21. Neil Bergmann, Peter J. Robinson, Server-Based Internet of Things Architecture, The 9th Annual IEEE Consumer Communications and Networking Conference, Brisbane, Australia, pp: 360 – 361, China, 2012.
22. Botterman M., 2009. for the European Commission Information Society and Media Directorate General, Networked Enterprise & RFID Unit – D4, Internet of Things: An Early Reality of the Future Internet, Report of the Internet of Things Workshop, Prague, Czech Republic.
23. INFSO D.4 Networked Enterprise, RFID INFSO G.2 Micro & Nanosystems, in: Co-operation with the Working Group RFID of the ETP EPOSS, 2008. Internet of Things in 2020, Roadmap for the Future, Version 1.1.
24. Vilamovska A, Hattziandreu, E., et al., 2009. RFID Application in Healthcare – Scoping and Identifying Areas for RFID Deployment in Healthcare Delivery, RAND Europe.
25. Lakshman T., Madhow U, 1997. The performance of TCP/IP for networks with high bandwidth-delay products and random loss. IEEE/ACM Transactions on Networking 5 (3) Pages: 336–350.
26. Jules A., 2006. RFID security and privacy: a research survey. IEEE Journal on Selected Areas in Communications, 24 (2), Pages: 381–394.
27. Lu T.,Neng W., 2010. Future Internet: The Internet of Things. IEEE International Conference on Advanced Computer Theory and Engineering (ICACTE), China, Pages: 376-380.
28. Odrigo R., Cristina A., 2011. Key management systems for sensor networks in the context of the Internet of Things. Elsevier, Computers and Electrical Engineering, Article in Press.
29. Sachin Babar, Parikshit Mahalle, Antonietta Stango, Neeli Prasad and Ramjee Prasad, 2010, Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT). Springer
30. Nilssen A., 2009. Security and privacy standardization in internet of things, in: eMatch. 09 – Future Internet Workshop, Oslo, Norway.
31. Eschenauer L., Gligor V., 2002. A key-management scheme for distributed sensor networks.

The Ninth ACM Conference on Computer and Communications Security, Washington, DC, USA.

32. Chenghua Yan, Kun Feng, Zhiming Zhang, Impact of Internet of things on security grade evaluation, International Conference on Computer Science and Electronics Engineering, PP: 289 – 292, China, 2012.

33. Chan H., Perrig A., 2003. Security and privacy in sensor networks, IEEE Computer 36 (10) Pages: 103–105.

34. Weber R., 2010. Internet of Things – New security and privacy challenges. Elsevier Computer Law and Security Review, Volume 26, Pages 23-30.

35. Jie Liu, Xu Hu, Zhiqiang Wei, Dongning Jia, Chao Song, Location privacy protect model based on positioning middleware among the internet of things, International Conference on Computer Science and Electronics Engineering, pp: 288 – 291, China, 2012

36. Hui Suoa,, Jiafu Wan, Caifeng Zoua, Jianqi Liua, Security in the Internet of Things: A Review, IEEE International Conference on Computer Science and Electronics Engineering, pp: 648-651, Zhejiang, China, 2012

37. Dunkels A., Vasseur J., 2008. IP for Smart Objects, Internet Protocol for Smart Objects (IPSO) Alliance, White Paper #1. http://www.ipso-alliance.org.

38. Hui J., Culler D., Chakrabarti S., 2009. 6LoWPAN: Incorporating IEEE 802.15.4 Into the IP Architecture – Internet Protocol for Smart Objects (IPSO) Alliance, White Paper #3, January 2009, http:// www.ipso-alliance.org.

39. Kushalnagar N, Montenegro G., Schumacher C., 2007. IPv6 Over Low Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals, IETF RFC 4919.

40. Y.-W. Ma, C.-F. Lai, Y.-M. Huang, J.-L. Chen, 2009. Mobile RFID with IPv6 for phone services, in: Proceedings of IEEE ISCE, Kyoto, Japan.

41. S.-D. Lee, M.-K. Shin, H.-J. Kim, 2007. EPC vs. IPv6 mapping mechanism, in: Proceedings of Ninth International Conference on Advanced Communication Technology, Phoenix Park, South Korea.

42. Minkeun Ha, Seong Hoon Kim, Hyungseok Kim, Kiwoong Kwon, Nam Giang, and Daeyoung Kim, SNAIL Gateway: Dual-mode Wireless Access Points for WiFi and IP-based Wireless Sensor Networks in the Internet of Things, The 9th Annual IEEE Consumer Communications and Networking Conference - Smart Spaces and Personal Area Networks, , Page(s): 169 – 173, Daejeon, Korea, 2012

43. Shancang Li, Da Xu, and Xinheng Wang, 2012, Compressed Sensing Signal and Data Acquisition in Wireless Sensor Networks and Internet of Things, IEEE Transactions on Industrial Informatics, Issue: 99.

44. Zhanjie W., Guoyuan M., Keqiu L., 2010. Research on the Real-time of the Perception between Objects in Internet of Things based on Image. The Fifth IEEE Annual ChinaGrid Conference, China, Pages: 92-97.

45. Runian L, 2009. Study on the Internet of Things Based on RFID Technique," Journal of CAEIT, 6(4):pp.594-597.

46. Hao W, 2009. RFID, EPC and Things of Internet. Radio Frequency Identification Technologies and Applications: Pages:17-20.

47. Chen D., Varshney P., 2004. QoS support in wireless sensor networks: a survey, in: International Conference on Wireless Networks 2004, Las Vegas, NE, USA.

48. Harald S., Patrick G., Peter F., Sylvie W., 2010 .Vision and Challenges for Realising the Internet of Things. Cluster of erponean research projects on the Internet of Things.

49. Cooper J, 2009. A. Challenges for Database Management in the Internet of Things. IETE Tech Rev, 26:320-9.

50. Xiaolei Li, Jiawei H., Sangkyum K., 2007. Hector G., ROAM: Rule- and Motif-Based Anomaly Detection in Massive Moving Object Data Sets. SDM.

51. J.-G. L., Han J., and X. Li. 2008. Trajectory outlier detection: A partition-and-detect framework," Proc. 24th Int'l Conf. on Data Engineering, pages140-149, Cancun, Mexico.

52. Jae-Gil L., Jiawei H., Xiaolei L., Hector G.: 2008. TraClass: trajectory classification using hierarchical region-based and trajectory-based clustering. PVLDB 1(1): 1081-1094.

53. Jae-Gil Lee, Jiawei Han, Kyu-Young Whang. 2007. Trajectory clustering: a partition-and-group framework. SIGMOD 593-604.

54. Joydeep G, 2007. Probabilistic Framework for Mining Distributed Sensory Data under Data Sharing Constraints. First International Workshop on Knowledge Discovery from Sensor Data.

55. James A., Cooper J., Jeffery K., Saake G. 2009. Research Directions in Database Architectures for the Internet of Things. A Communication of the First International Workshop on Database Architectures for the internet of things, Pages: 225-233.

56. Shen Bin, Liu Yuan, Wang Xiaoyi, 2010. Research on Data Mining Models for the Internet of Things. International Conference on Image Analysis and Signal Processing (IASP), Pages: 127 – 132, Zhejiang, China.

57. Kiritsis D., 2010. Closed-loop PLM for intelligent products in the era of the Internet of Things. Elsevier, In press.

58. Gerd K., Fahim K., Daniel F., Vasughi S., 2010. Smart Objects as Building Blocks for the Internet of Things. IEEE Internet Computing, vol. 14, no. 1 pages: 44-51.

59. Ma Y., Lai C., Y., M. Huang M, J., Chen L., 2009. Mobile RFID with IPv6 for phone services. IEEE ISCE, Kyoto, Japan.

60. S.-D. Lee, M.-K. Shin, H.-J. Kim, 2007. EPC vs. IPv6 mapping mechanism. Ninth International Conference on Advanced Communication Technology, Phoenix Park, South Korea.

61. D.G. Y, D.H. Lee, C.H. Seo, S.G. Choi, 2008. RFID networking mechanism using address management agent, in: Proceedings of NCM, Gyeongju, South Korea.

62. <http://ipv6.com/articles/applications/Using-RFID-and-IPv6.htm>.

63. Vasseur J., Dunkels A., 2010. Chapter 4 - IPv6 for Smart Object Networks and the Internet of Things, Elsevier Interconnecting Smart Objects with IP, Pages: Pages 39-49.

Conceptual Model of Real Time Infrastructure Within Cloud Computing Environment

AAmir Shahzad aamir@unikl.edu.com.my
Malaysian Institute of Information Technology (MIIT)
University Kuala Lumpur,Malaysia

Shahrulniza Musa shahrulniza@miit.unikl.edu.my
Malaysian Institute of Information Technology (MIIT)
University Kuala Lumpur,Malaysia

Abdulaziz Aborujilah abdulazizh@unikl.edu.my
Malaysian Institute of Information Technology (MIIT)
University Kuala Lumpur,Malaysia

Mohd Nazri Ismail mnazrii@miit.unikl.edu.my
Malaysian Institute of Information Technology (MIIT)
University Kuala Lumpur,Malaysia

Muhammad Irfan irfanview2@yahoo.com
Windfield College,
Kuala Lumpur,Malaysia

Abstract

Cloud computing is a new and most demandable technology in communication environment. Where computing resources such as hardware or/and software are processed as service over networks. SCADA implementation within cloud environment is relatively new and demandable over real time infrastructure (industrial infrastructure).The shifting (moving) of SCADA system (applications and resources) within cloud based infrastructure,meanfully overcome the cost and improve the reliability and performance of whole system. Cloud computing provides on-demand network access and batch of computing services for SCADA system. The current research paper takes two conceptual ideas to implement SCADA system within cloud computing (Hybrid Cloud) environment. In the first phase, SCADA applications are processed entirely inside the hybrid cloud. In the second phase, SCADA applications are running in separate application server directly connected to devices in a SCADA network and rest of paper discusses the security related to SCADA and cloud computing communication.

Keywords: Cloud Computing, SCADA (Supervisory Control and Data Acquisition), Prevention and Detecteion System,Security attack/issues.

1. INTRODUCTION

“Supervisory control and data acquisition (SCADA) system has been deployed/implemented over several real time infrastructures and the field devices that are connected within network(LAN/WAN) are control and monitor from central location (SCADA master station). Supervisory control and data acquisition (SCADA) system architecture has five main components such as master station, remote station, user interface/human machine interface (HMI), Historian/database, and communication media (network), these are used to provide communication within SACDA system” [8],[11].

Information Technology industry is becoming broader and used in many areas of daily life activities. Cloud computing as one of new IT Models is widely used in different area including software and hardware delivery model. Cloud computing provides end users with fixable and scalable sharable computing services. In study [1], for application development process, the developers no need to own all requirements of application building. Instead of that they can use well established development environment available in the cloud (PaaS) platform as service [2]. GAE, Microsoft Azure are some PaaS example .Similarly, several tenants are able to share same application software simultaneously based on payment as usage agreement [3], which called (SaaS) software as a service [4]. In addition to that, using computing Infrastructure resources is available on cloud Infrastructure as a service (IaaS)[3]. This can provide end users with latest computing technologies based on client and provider agreement .PaaS provider such as GoGrid, Flexiscale, and Layered Technologies etc. Cloud deployment model is divided into four models, public, private, community and hybrid. In public the cloud services offered by third-party provider who own the cloud infrastructures. Moreover, end users are able to utilize cloud services located in Off-premise location. The main disadvantage (drawback) in public cloud model is weakness of access security model[5].In private and hydride cloud, cloud services can offered by the origination or by third party and the same thing for cloud Infrastructure ownership. Cloud services can be Off-premise or On-premise. The main advantage in this model; resources access and consumption are more trustable than public[5].

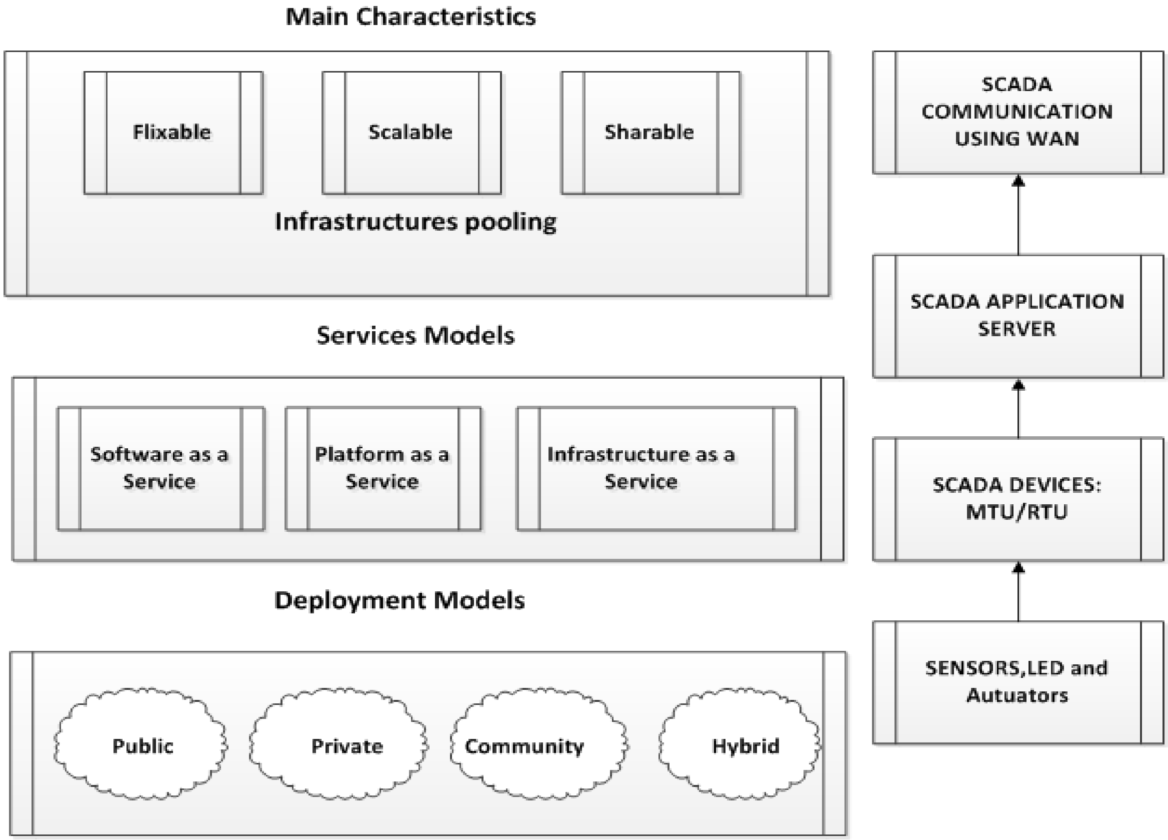

FIGURE 1: SCADA and Cloud Architecture.

2. LITERATURE REVIEW

“Greenville Utilities Commission (GUC)” [1], they suggest integration of SCADA with open cloud technology which give a new opportunity to current business to add new value to their investments and increase their productivity . They can get more benefit from historical data existed in cloud to make their business more successful and more concurrent about OS and platform SCADA (in cloud).This also help GIS to get real time SCADA map, and help also LIMS to obtain real time report to their laboratory data and SCADA process and help also CMMS systems to organize maintenance works based on real time data and end customers can get their SCADA invoice easily using cloud. When several of SCADA system is sharing infrastructure on cloud that can reduce the cost of all single system infrastructures. SCADA in cloud give a Decision-makers vision about computation of real time data weather forecasting and electrical usage rate to make decisions and thus reducing the cost.

In [2], Smart grid is kind smart electrical networks, it use IS (Information system) to enhance its effectiveness. It give consumers kind of connectivity. Using smart grid applications in cloud is discussed. The security is one of challenges to involve smart grid in cloud so, paper has proposed a frame work to handle this problem.

In[3] , the paper argue that there is an urgent need to scalability features in Smart Grid management . The cloud computing paradigm is able to offer this feature but it still suffers from some shortages. The most important one is security obstacles. Moreover, the paper also argues that when this problem is solved smart grid management system in the cloud can be more effective.

“VS-Cloud” has been proposed to shift SCADA system within cloud computing environment for SCADA efficiency enhancement and for the purpose of reliability, but security is the major problem consider within communication [4]. The results have been captured, based on power consumption and cloud architecture performance in power system within grids network communication [5].

In [6], SCADA applications(softwraes) are completely install within cloud computing environment rather than traditional computer system.No longer need to update computing resources in case of needs instead cloud infrastructure can be used. In addition, with cloud cost of IT staff can be reduces as well. SCADA Staff collaboration can be easily done in cloud regardless of the time and location of communicating. However, some of obstacles is still in cloud which make many reluctant to use SCADA in cloud such as reliability, security, performance challenges. Some of security risk such as lack in privacy and weakness in performance such as bandwidth overload and latency cased by losing internet connection.

In [7], Microsoft has proposed to oil and gas company using a new cloud based SCADA system. This system connected with HMI station and RTU terminal. It also includes online cloud based SCADA system offering end user with historical data. End can user just kind of thin client station to get a required report in easy way. This system offer high reliability through databases redundancy and synchronously.

Cryptography solution has been successfully implemented “between master terminal unit (MTU) and remote terminal units (RTUs) and/or remote terminal units (RTUs) and master terminal unit (MTU)”. The implementation successfully achieved the security services and overcomes the attacks related with SCADA communication [9]. Another research also successfully implemented the cryptography solution within the layers (application layer and data link layer) of distributed network protocol (DNP3). The implementation within DNP3 layers successfully enhance the SCADA security, achieved the security services and minimized the attacks ratio of DNP3 as part of SCADA system [11].

3. CONCEPTUAL IMPLEMENTATION

A proposed conceptual idea, used to connect Malaysian eight states ports such as Johor, Kedah, Kelantan, Malacca, Pahang, Perak, Penang and Terengganu together connected with head quarter which is located in Kuala using hybrid cloud computing infrastructure. These ports are based on SCADA implementation using TCP/IP connectivity with WAN or Internet.

Each port has an own private cloud and every cloud is connected with headquarter cloud (public cloud) in Kuala Lumpur, same as distributed SCADA application in cloud infrastructure. In first phase illustrated in figure 2; all SCADA applications (such as HMI software, reporting, monitoring, visualization and execution etc) are processed entirely inside cloud and simultaneously all processing will save in headquarter (Kuala Lumpur) for monitoring and backup storage using WAN and allow remote user to interact with SCADA. Each time when communication will occur between Master Terminal Unit and Remote Terminal Unit are preceding using cloud [10]. In the second phase illustrated in figure 5, SCADA applications are running in separate application server directly connected to devices in SCADA network [10], and send Information to cloud for monitoring and storage and simultaneously all processing will save in headquarters (Kuala Lumpur). SCADA implementation within cloud computing is new technology and processing is quite different from traditional networks. SCADA solution providers and users have adopted this technology to save costs, scalability, reliability, and enhance performance results. Security is a big issue in SCADA within the cloud as compared with traditional networks because of SCADA

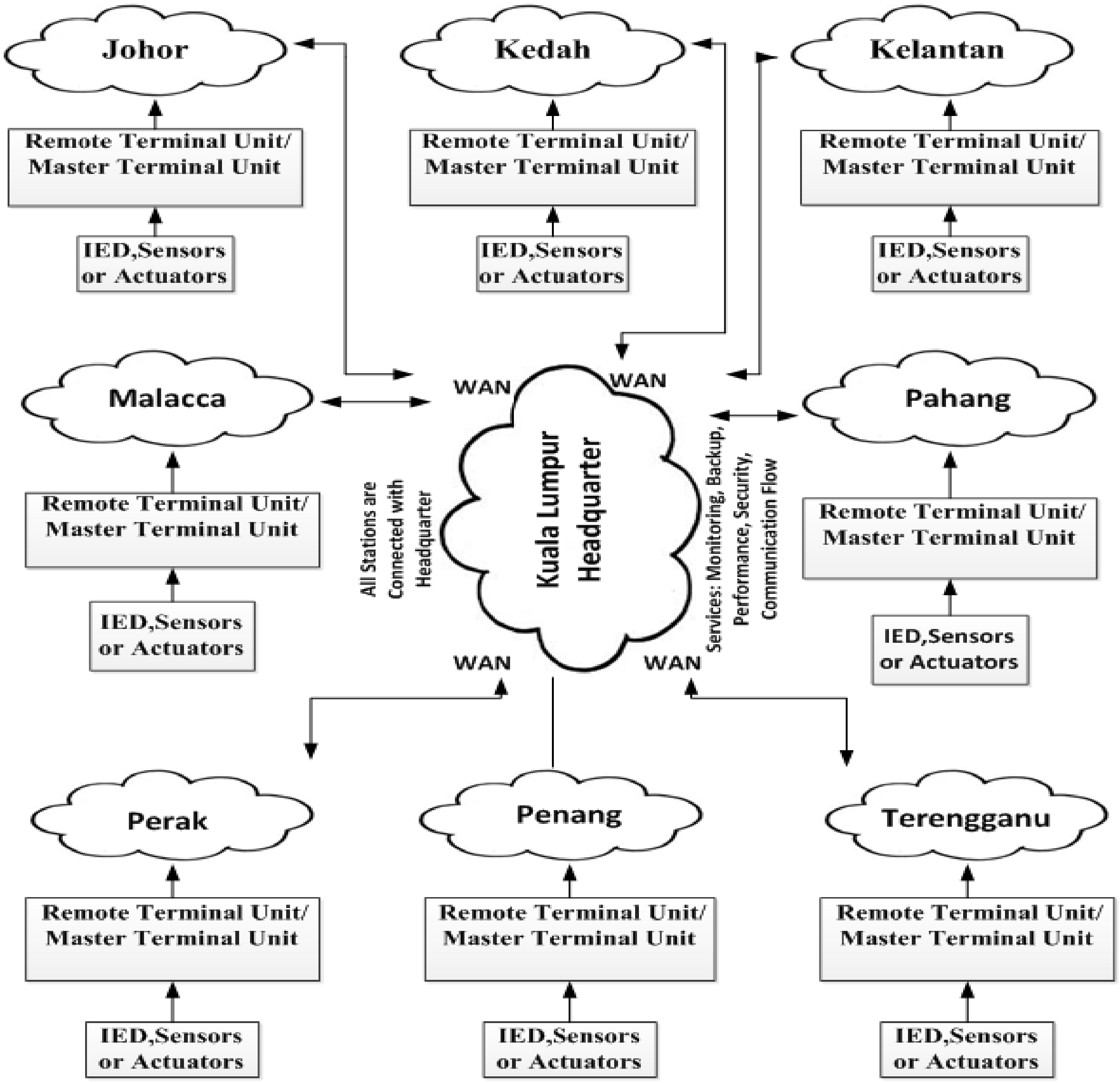
Johor
Kedah
Kelantan
Remote Terminal Unit/ Master Terminal Unit
IED,Sensors or Actuators
Malacca
Pahang
WAN
WAN
WAN
WAN
Kuala Lumpur Headquarter
All Stations are Connected with Headquarter
Services: Monitoring, Backup, Performance, Security, Communication Flow
Perak
Penang
Terengganu

FIGURE 2: Cloud Base SCADA System (Phase 1).

systems are based on real time delivery of message/data but the TCP / IP protocol doesn't provide functionality related to real time Message delivery such as DNP3, Modbus, Field bus and other SCADA protocols.

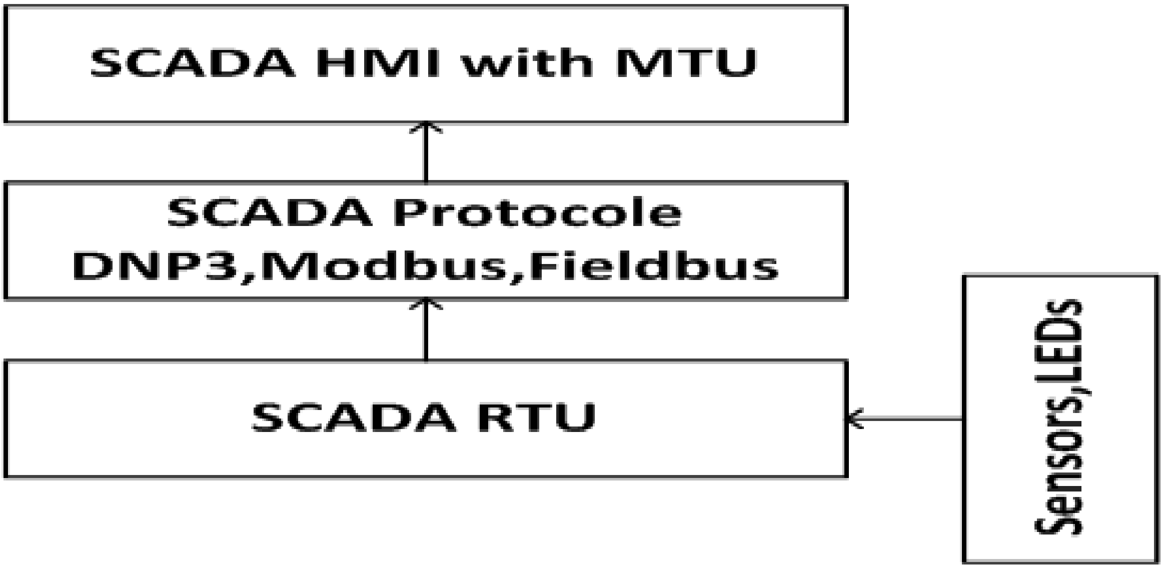

FIGURE 3: SCADA Communication.

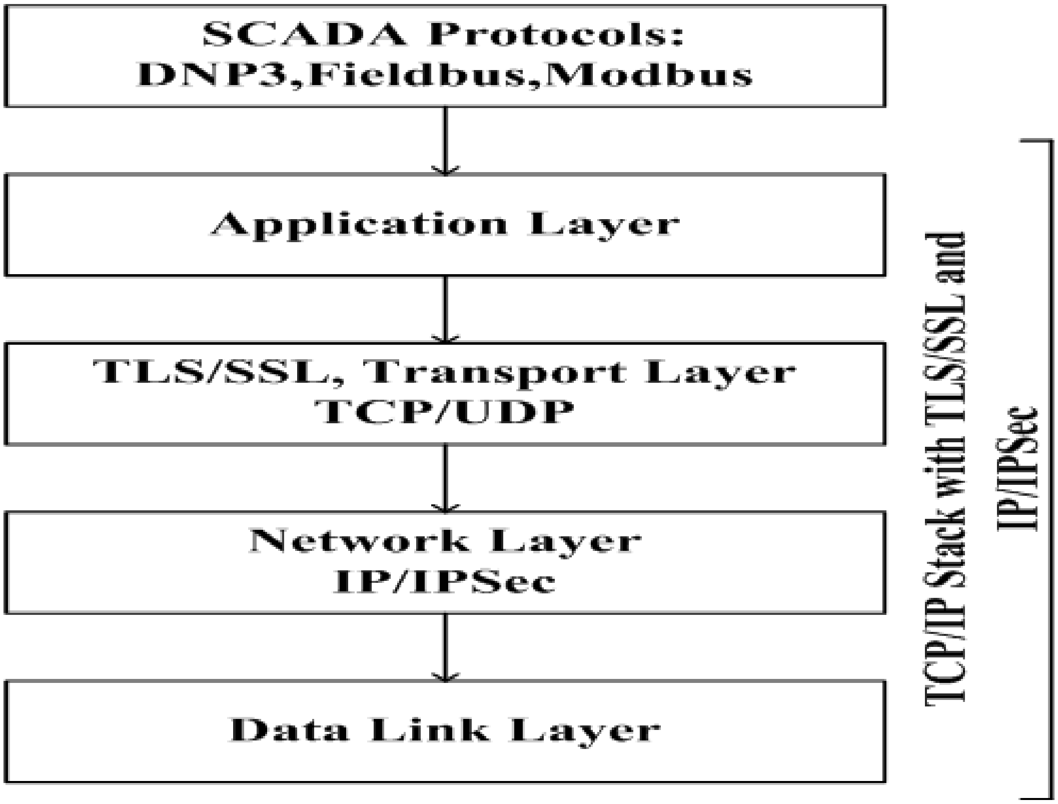

FIGURE 4: SCADA Communication with TCP/IP Stack.

Each private cloud and headquarter cloud (public cloud) Uses SSL/TLS in their communication (Illustrated inFigure 4). However, the SSL / TLS protocol has limitations because the SSL / TLS protocol relies on transport protocols such as TCP/IP, and cryptography and signature algorithms for security purposes. So, the best solution / approach is to be used Cryptography or signature algorithms to secure SCADA communication within the cloud. Figure 3 illustrated the simple SCADA architecture connected with the MTU / RTU

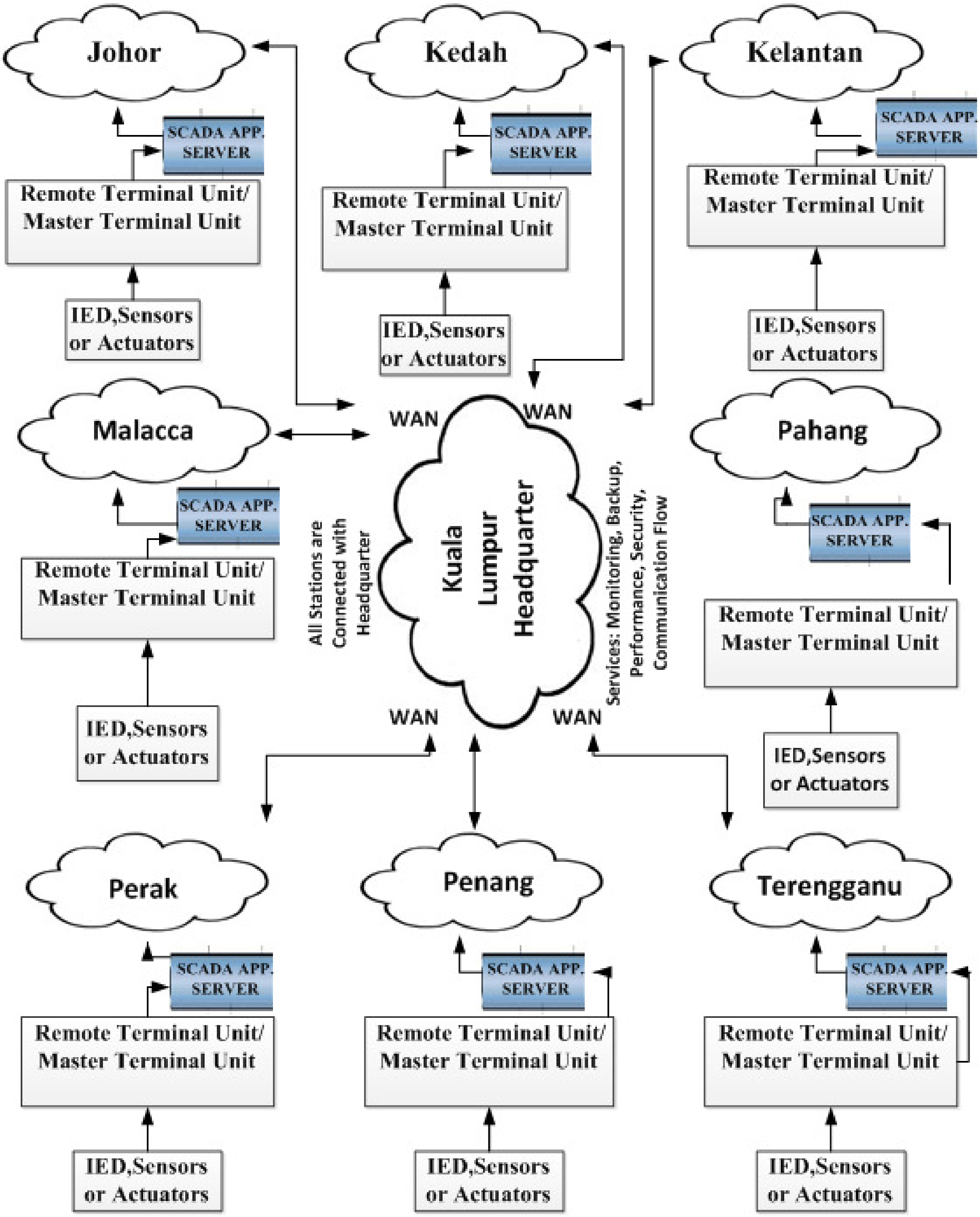
Johor
Kedah
Kelantan
Malacca
Pahang
Perak
Penang
Terengganu
SCADA APP. SERVER
Remote Terminal Unit/ Master Terminal Unit
IED,Sensors or Actuators
WAN
Kuala Lumpur Headquarter
All Stations are Connected with Headquarter
Services: Monitoring, Backup, Performance, Security, Communication Flow

FIGURE 5: Cloud Base SCADA System (Phase 2).

4. CONCLUSION and FUTURE WORK

The implementation within cloud computing is new and demandable over real time infrastructure. Using cloud environment, SCADA overcomes the cost and improve the reliability and performance but the same time current platform has a lot of risks and security issues related to detection and prevention inside communication. Current research using SCADA within cloud environment ;gives new research direction for implementation of our proposed framework in real environment and directions to secure SCADA communication within cloud using TLS/SSL and more advance to apply cryptography and covariance mathematical model .

5. ACKNOWLEDGMENTS

We are sincerely and heartily grateful to our supervisors Assoc .Prof.Dr.Shahrulniza Musa and Dr. Mohd.Nazri Ismail for the support and guidance they showed us throughout our research paper writing. We are sure it would have not been possible without their help. Besides we would like to thank to our parents and our friend, Irfan boosted them morally and provided us great information resources.

6. REFERENCES

1 Langley, R. and M.J. Moreau, SCADA – Mining Value Beyond Process Control Ricky Langley, Advanced Enterprise Systems Corporation (AESC), 740 SE Greenville Blvd. STE400 BOX323 Greenville, NC 27858.

2 Fayyaz, S. and M.M. Nazir, Handling Security Issues for Smart Grid Applications using Cloud Computing Framework. Journal of Emerging Trends in Computing and Information Sciences, 2012. 3(2).

3 Birman, K.P., L. Ganesh, R. van Renesse, Running Smart Grid Control Software on Cloud Computing Architectures, 2011.

4 Alcaraz, I.A , David Nu˜ ez, J. L,Managing Incidents in Smart Grids a la Cloud Cristina.

5 Geberslassie, M. and B. Bitzer, Cloud Computing for Renewable Power Systems.

6 White Paper Cloud-Based SCADA Systems: The Benefits & Risks Is Moving Your SCADA System to the Cloud Right For Your Company.

7 Global Energy forum 2012, Cloud Based SCADA system for the Oil and Gas Industry.

8 www. wikipedia.org

9 S. Musa, A. Shahzad, A.Aborujilah,Simulation base implementation for placement of security services in real time environment, Proceeding ICUIMC '13 Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication.

10 Cloud Computing for SCADA, http://www.controleng.com.

11 S. Musa, A. Shahzad, A.Aborujilah, Secure security model implementation for security services and related attacks base on end-to-end, application layer and data link layer security, Proceeding ICUIMC '13 Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication.

INSTRUCTIONS TO CONTRIBUTORS

The International Journal of Computer Networks (IJCN) is an archival, bimonthly journal committed to the timely publications of peer-reviewed and original papers that advance the state-of-the-art and practical applications of computer networks. It provides a publication vehicle for complete coverage of all topics of interest to network professionals and brings to its readers the latest and most important findings in computer networks.

To build its International reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCN.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Started with Volume 5, 2013, IJCN aims to appear with more focused issues. Besides normal publications, IJCN intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

We are open to contributions, proposals for any topic as well as for editors and reviewers. We understand that it is through the effort of volunteers that CSC Journals continues to grow and flourish.

IJCN LIST OF TOPICS
The realm of International Journal of Computer Networks (IJCN) extends, but not limited, to the following:

- Algorithms, Systems and Applications
- ATM Networks
- Cellular Networks
- Congestion and Flow Control
- Delay Tolerant Networks
- Information Theory
- Metropolitan Area Networks
- Mobile Computing
- Multicast and Broadcast Networks
- Network Architectures and Protocols
- Network Modeling and Performance Analysis Network
- Network Security and Privacy
- Optical Networks
- Personal Area Networks
- Telecommunication Networks
- Ubiquitous Computing
- Wide Area Networks
- Wireless Mesh Networks
- Ad-hoc Wireless Networks
- Body Sensor Networks
- Cognitive Radio Networks
- Cooperative Networks
- Fault Tolerant Networks
- Local Area Networks
- MIMO Networks
- Mobile Satellite Networks
- Multimedia Networks
- Network Coding
- Network Operation and Management
- Network Services and Applications
- Peer-to-Peer Networks
- Switching and Routing
- Trust Worth Computing
- Web-based Services
- Wireless Local Area Networks
- Wireless Sensor Networks

CALL FOR PAPERS

Volume: 5 - Issue: 3

i. Submission Deadline : November 30, 2013 **ii. Author Notification:** December 25, 2013

iii. Issue Publication: December 2013

CONTACT INFORMATION

Computer Science Journals Sdn BhD
B-5-8 Plaza Mont Kiara, Mont Kiara
50480, Kuala Lumpur, MALAYSIA
Phone: 006 03 6207 1607
006 03 2782 6991

Fax: 006 03 6207 1697

Email: cscpress@cscjournals.org

CSC PUBLISHERS © 2013
COMPUTER SCIENCE JOURNALS SDN BHD
B-5-8 PLAZA MONT KIARA
MONT KIARA
50480, KUALA LUMPUR
MALAYSIA

PHONE: 006 03 6207 1607
006 03 2782 6991

FAX: 006 03 6207 1697
EMAIL: cscpress@cscjournals.org