Indonesian Journal of Electrical Engineering and Computer Science
Vol. 2, No. 1, April 2016, pp. 229 ~ 240
DOI: 10.11591/ijeecs.v2.i1.pp229-240

Applications and Design for a Cloud of Virtual Sensors

Ammar Jameel Hussein*[1], Ammar Riadh[2], Mohammed Alsultan[3], Abd Al-razak Tareq[4]
[1]Çankaya University, Turkey, Ankara,
[2]Baghdad Unvercity, Baghdad, Iraq,
[3]Çankaya University, Turkey, Ankara,
[4]University of Technology, Baghdad, Iraq,
Corresponding author, e-mail:ammar.jameel.ict@gmail.com[1], eng_ammar81@yahoo.com[2], mohammed.altaliby@gmail.com[3], abdtareq@yahoo.com[4]

Abstract

The use of sensors in our daily lives is a growing demand with the large number of electronic devices around us. These sensors will be included in our daily life requirements soon and they will affect our lives in both positive and negative ways. In this paper, we discuss the manner, applications and design issues for a cloud of virtual sensors, and we introduce a distributed system design to deal with physical sensors that reside in diverse locations and operate in different environments. This design operates in a cloud computing vision and can make virtual sensors in upper of physical one available from anywhere using ICT structure. Then, we negotiated the future of this technology, i.e., the Internet of Things (IoT). Additionally, we go over the strengths and weaknesses of using this technology. Our test lab shows high performance and good total cost of ownership and effective response time.

Keywords*: Cloud Virtual Sensors, Internet of Things (IoT), Sensor Cloud, Virtual Sensor, weir less sensor network*

1. Introduction

The main Physical sensors are used all around the world in numerous applications [1]. For the most part, sensors are regularly used by their own applications since each application retrieves data entirely with the cooperation of physical sensors and their sensor statistics. Additionally, vendor requests cannot be customized to the physical sensors in a diverse event [2]. Perhaps this is one of the main reasons that give us a new concept of the need forvirtual sensors [3] and a sensor cloud [4]. A sensor cloud can be defined as a collection ofvirtual sensors comprised of physicalsensors. Consumers inevitably and dynamically can establish or deliver on the basis of application demands. This method has a number of advantages.

Firstly, this improves sensor administration capability. Consumers can use devices regarding their view of wireless sensor networks (WSN), typical tasks for a varietyof factors include area of interest, security and latency. Secondly, statistics attained by WSN can be public among many consumers, which can reduce the totalcost of data gathering for both an organization and the customer.

As a result, many of the effective power performance methods have improved and almost all protocols that have been used in sensor networks are enhanced to decrease power feeding. These improvements include working in different layers, including the Transport Layer, the Network Layer, the Physical Layer and the Medium Access Control Layer. In the meantime, the communicating process needs extra power relative to the data process handling tasks. A variety of additional machineries have been suggested and improved to save power. These include external-network handling [1], topology restructuring, Time Synchronization and Node Architecture [4].

Correspondingly, the security and privacy of a sensor node and communications line is also a major standing issue in the sensor network [2]. Sensing and carrying data more often has its own private use and nature. Many challenges in this aspect have been issued. Furthermore, many proposals for solutions have been applied, including cryptography and steganography. However, such techniques are extremely costly to be implanted in such devices, i.e., time considerations, especially in real-time applications. Others have suggested solutions that include adding security information hooked on to the data packet. Again, this will cost in terms of

Received January 7, 2016; Revised March 18, 2016; Accepted March 28, 2016

processing and memory. Lastly, another aspect of the challenge in sensor networks can be the availability and operational costs as a result of unreliable communications lines, environmental conditions and restrictions of energy sources.

While sensor-cloud is trying to virtualizes the physical sensor by way of putting them on the cloud dynamically, Grouping these sensors in virtual manner and putting them in cloud computing can be available on demand when other applications need them, and from this concept, a new term is found: “Internet of Things” (IoT), which proposes the potential of assimilating the digital domain of the Internet with the physical domain in which we breathe [5].

In order to realize this proposal, we need to demand a systematic method for assimilating sensors, the operator and the information on which they operate on the Internet we see nowadays. In this paper, we will discuss the virtual sensor, sensor clouds and the Internet of Things. We will review issues and applications of a cloud of virtual sensors, introduce a design for a virtual cloud sensor and finally overview the pros and cons of this technology.

2. Virtual Sensor

A virtual sensor is the emulation of a physical sensor that obtains its own data from underlying physical sensors. Virtual sensors provide a customized view to users using distribution and location transparency [6]. Virtual sensors contain meta-data about the physical sensors. The required physical sensors should be dynamically organized in the following order: virtualization, standardization, automation, monitoring and grouping in the service model.

Implementation of virtual sensors is carried out in four different configurations: one-to-many, many-to-one, many-to-many, and derived configurations [7]. In the following parts, there are brief reviews ofeach structures:

1) One-to-Many Structure: This structure deals with one physical sensor link to several virtual sensors.
2) Many-to-One Structure: In this structure, the topographical areas are allocated into zones and each zone can have one or more physical sensors and sensor networks.
3) Many-to-Many Structure: This configuration is a combination of the one-to-many and many-to-one configurations. A physical sensor can correspond with many virtual sensors and also be a part of a network that provides aggregate data for a single virtual sensor.
4) Derived Structure: A derived configuration refers to a versatile configuration of virtual sensors derived from a combination of multiple physical sensors. In the derived configuration, the virtual sensor communicates with multiple sensor types while the virtual sensor communicates with the same type of physical sensor in the other three configurations. Figure 1 shows the different structure schema.

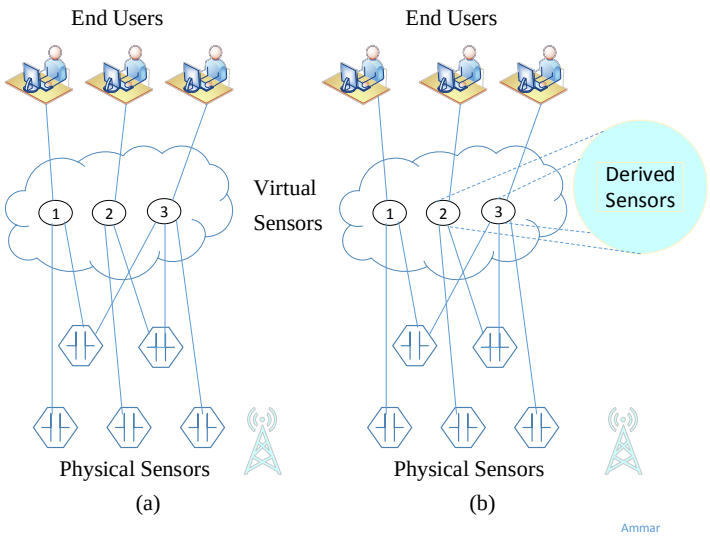

Figure 1. Virtual sensors structure schema

3. Sensor Cloud

A sensor cloud can be derived from the following definition: a structure that permits real universal calculation of data using virtual sensors as an edge among physical sensors using an Internet cloud network[8]. Statistics are calculated through servers to cluster infrastructure with the cyber network as the communication medium. These methods will enable consumers effortlessly to access, handle, visualize and evaluate, in addition to load, allocate and examine huge numeral data from a sensor. Data is gathered from more than a few types of applications, and this large sum of data are visualized by expending the IT and storage resources in cloud computing. The idea of a virtual sensor cloud is a model that combines the idea of a virtual sensor and cloud-computing. Physical sensors (WSN) gather statistics and conduct whole sensor data into a cloud-computing frame. Cloud-sensors can grab sensor data resourcefully and use this data to monitor numerous applications. The cloud service structure is used to distribute the facilities of shared virtual network services in which consumers/end user's benefit by using these services. They are notworried about how they are detailed to implement the service. This is referred to as transparency and scalability.

4. Internet of Things (IOT)

In order to access object or things from anywhere, it is a different idea from the concept of cloud sensors. Access these virtual sensors via the cloud service in our proposed design; it is called a cloud sensor. In fact, there is another concept that is nested within our subject, namely the "Internet of Things" (IoT). It is stated that if objects, individuals or things provide an exclusive ID, they will have the capability robotically to transmit statistics through networks withoutneeding a human or non-human/computer interface. IoT has grown from the union of (WSN) technology and micro electromechanical systems (MEMS) by using the Internet [9] [10].

Furthermore, the term "thing" in this sense may mean someone with an implant heart sensor, animals, plants, etc. This may refer to any component that has been integrated by sensors and making the driver be aware of changes in speed or any other expected measurement. Additionally, it may be any items with the capability of allocating IP addresses and delivering statistics through a network. Figure 2 symbolizes the "IoT."

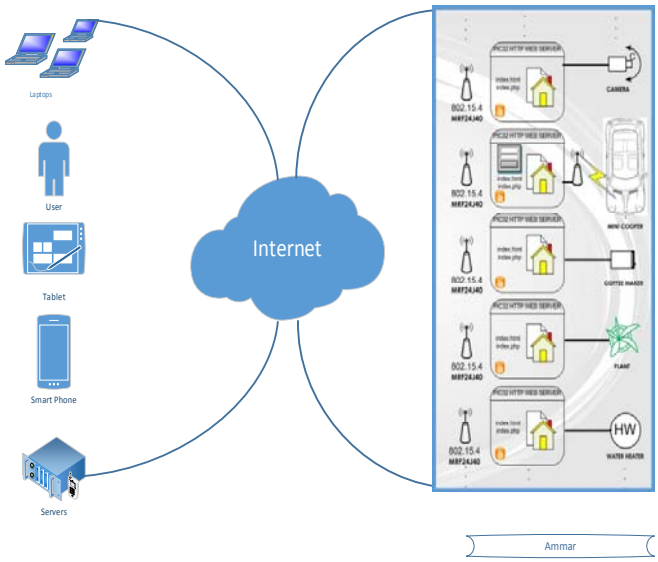

Figure 2. IoT

The idea behind theInternet of Things, is all about embedding microprocessors in objects, hence, they can communicate with each other. The information will lead us in the future to a new term called the Internet of everything.

4.1 Things That Think

Things in the context of the Internet of Things can be any object, smart devices, entities that can be linked to a network and provide information regarding the purpose for which it was designed whether with or without computing abilities [16]. Usually these objects have mobile ability and can be active or passive power sources. Some objects have their own batteries and others are powered by sources from the environment and natural surroundings, such as light, water, heat, etc. Mobility denotes a communication link between an object and the main station or nodes that are wireless [27].

4.2 Internet of People

The Internet of people (IoP) [17] is a new developed paradigm that attempts to extend the usage of the Internet of Things by involving the things around people so as to interact with them positively and meaningfully in their normal daily lives.In the Internet of Things, the main goal of integrating things is to have these things become involved in our life and to make them more easily accessible for the consumer by having a machinery model work for them effortlessly. On the other hand, the Internet of People suggested that these things can analyze data and make decisions depending on data acquired from consumers themselves and then respond to these data accordingly.

4.3 The Web of Things

The Web of things (WoT) is a new paradigm that attempts to extend the concept of the Internet of Things. The Web of Things is an impression of typical lives that assumes that conventional objects and sensors are fully connected and integrated using Web 2.0 technology [18]. The Web of Things presents several benefits in web society and has suggested a new web application paradigm. These applications can be simply built on top of objects using Web development utilization; this may include blogging, securing, searching, linking, caching, etc. The Web of Things paradigm provides a scalable and remarkable model and because of this, some researchers have faith that this model will be suitable for connecting objects in uniform edges and be simply applied by following these steps:

1. Linking the object to the Internet by using IPv4 or IPv6
2. Enabling a Web service on these objects
3. Utilizing these services and putting them into the Web model
4. Representing these services as Web resources

Essentially, the Web of Things process can be achieved in two different ways: the first method includes enabling web services with an object or by deploying another device to act as a gateway. The main objective of this gateway is protocol conversion from TCP/IP protocols to the protocol being used by a specific object, including ZigBee, Bluetooth, etc. Gateway methods are preferred as it is not likely to attach a TCP/IP stack within objects, such as barcodes and RFID tags [19]. A new study [20] on the issues in the Web of things discusses the global detection of objects; Web services enablers in objects, time synchronizations, interaction through the web and language standardization.

5. Sensor Cloud Application

There are many applications that use the concept of cloud sensors. The four main categories include the following [11]:

1) Health Care: A cloud of virtual sensors can be used in the health care sector. In some new hospitals, physical and virtual sensor networks are commonly used to monitor patients' biological information, to switch drugs and to track and monitor patients and doctors within or outside a hospital.
2) Transportation Monitoring: A cloud of virtual sensors can be used also in transport monitoring systems by using basic administration systems such as traffic control, celestial navigation, car plate number deduction, emergency alarms, etc.
3) Military purposes: A cloud of virtual sensors can be used in many military applications such as following up friendly forces movement, action surveillance, exploration of enemy forces, determination of enemy pointing, war assessment and nuclear effects, anticipating and assessing biological and chemical attacks, etc.

4) Weather Prediction: The potential applications are very useful here to predict weather conditions and disasters such as tsunamis and earthquakes, volcanoes in addition to activity surveillance and expected effects, etc.

6. Sensor Network Security

Sensor networks usually have several restrictions similar to other network types. Therefore, it is not logical to implement a conventional security policy such as the traditional security steps [21] consequently, to build a security operational platform for the Internet of things; we need first to understand the nature of these restrictions on the form of the network. Some sensor network restrictions are briefly described below.

6.1 Limited Resources

Security mechanism procedures need a specific volume of resources to be available at least to implement this mechanism, including processing units to handle code, memory resources and power in sensor devices to carry out tasks in a timely manner. It is axiomatic that these resources are very scarce in the context of sensor networks. The two main restrictions are the power and memory needed [22].

6.2 Unreliable Communication

Implementation of security mechanism procedures hinges on the implementation of a set of protocols [22], which ultimately hinges on the reliability of the communication line within the network. This can break down the security mechanism in different ways.

- Unpredictable Communication links

Security network packets may be damaged, due to link errors packets dropped in high data traffic congested within the interior of the network.

- Interference

Wireless sensor networks use a space to broadcast and because of the nature of link competition, interference, collisions and crashes may occur in the wireless packets.

- Latency

Because of the load in data traffic and the process time needed, delays may occur in the sensor network. This will directly impact the security mechanism in real-time applications.

6.3 Unattended Operations

Wireless sensor networks are designed to operate in natural conditions [22], Sometimes these natural conditions may be beyond our control, including natural disasters, animal attacks, storms, etc. Therefore, physical attacks can occur in a sensor network.

7. Sensor Model and Standardization

In the present day, there are many efforts to characterize sensor data as standard data entities. This helps to build a based structure model for sensor systems. These new data representations attempt to produce a standardized model for sensor networks.This model can support diverse sensor applications to alter data effortlessly between sensor networks.

7.1 Sensor Web Enablement (SWE)

This first model was developed for this aspect, namely Sensor Web Enablement (SWE) standards founded by the Open Geospatial Consortium (OGC) organization [23], who formulated a set of standards/model and schema to gather so as to serve geographic interoperability. Sensor web enablement standards deliver essential structure encodings that permit a real-time combination of various sensors. Engineers, developers and application designers can use these standards to create their product platforms and applications. To enable the web in these devices, Open Geospatial Consortium members work with many services and encodings. SWE encoding includes Sensor Model Language (SensorML), Observations & Measurements (O&M), Transducer Model Language (TML) and SWE services which include the Sensor Observations Service (SOS), Web Notification Services (WNS), Sensor Alert Service (SAS), and Sensor Planning Service (SPS).

7.2 SensorML

Sensor Modeling Language (SensorML) [24] is a data model language similar to Extensible Markup Language (XML). SensorML attempts to offer a mechanism to describe the data of sensor systems and their communicator podiums. Every single sensor will be modeled as a functional operator that is an essential portion of the system. These essential operators cover input and output performance. The model metadata delivers information regarding measured phenomenon, calibration information, location information, time stamp for measurements, and the purpose of the measurement.

7.3 Sensor Observation Service (SOS)

This web service standard has been approved by the Open Geospatial Consortium [23] and describes a web service edge to enable detection and the retrieval of data in real-time applications. It is encoded in SensorML and measures values with O&M encoding.

8. Related Work

Javier Miranda, et al [12], proposed a smart architecture that is based on smart-phones as a way to interact with people who are involved in Internet of Things applications. The new things in this paradigm are the consideration of interacting and the adaptively between peoples and smart things in every day live by context of internet of things, This is an important idea that extends the use of Internet of Things applications and makes them smarter in people's everyday life activities. Moreover, they discuss the socially related issues of the impact on people to accommodate this transformation, i.e., from real life to smart life. Finally, they design middleware architecture that depends on this discussion and considers People as a Service (PeaaS) [13] and Social Devices.This layer has many components, including an action repository, application repository, a device registry and an application manager. This model gives the user the ability to build a social profile on their own devices and share this profile with the middleware layer, thereby enabling the adaptive reaction between things. Some weaknesses in this project include discussing issues out of the scope of the technology framework and assuming end-user interference as a part of this model.

Another study done by Sanjay Madria et al [14] proposed a new architecture for building a virtual sensor on top of the physical one. They discuss many components of this design. These architectures contain an intermediate layer between a sensor's device in the real world and consumers.The designed architecture includes three layers: a sensor-centric layer to deal with physical sensors; a middleware layer, intermediate layers; and a client-centric layer that handles the applications. In this design, it is not clearly shown how these layers can build a standard virtual sensor template on top of the physical one to handle different sensor types coming from different vendors and work using diverse technology.While Hoon-Ki Lee et al [15] proposed a new paradigm that enable the concept of the Social Web of Things (SoT), the paradigm was based on machine-to-machine talking in inspire the Web of Things. They implement a social sensor network that enables information associations in the context of web and social networks.The main component of this model includes the service domain, social relationships and user information. The main objective benefits of this model were finding a relationship between users, things and social networks and providing a dynamic service that has the ability to be reconfigured according to user needs and activities in the social network world. On the other hand, no security or privacy issues were discussed as a consequence of this wide sharing of information related to sensitive data, such as sensor networks.Moreover, Jih-Wei et al [25] introduced a new paradigm called "The Virtual Environment of Things (VEoT)." This paradigm aims to assimilate smart things in the real world with a virtual environment in the context of the Web of Things. In this project, they confirm the effectiveness of the model by designing a smart gateway and a core resource exchange. This core included a resource manager, an event manager and a smart object manager. The proposed model shows how the objects/things interacting with each other use real-time applications in the Web of Things environment. This project lacks standardization in the proposed design and they focused on software technologies instead of creating applications to serve the Web of Things.

9. Proposed Design

Our proposed design for a sensor cloud includes three main layers, each of which has a specific role and serves the up down layer. These layers can be classified thus:

1) Layer_1: This layer contracts with the preparation of the service template construction and provision standard definition in addition to defining the physical sensors as XML, web services or HTTP enabled. This will allow the service provider to access these sensors and develop them on several platforms without concern for the integration of a variance number of applications platforms.
2) Layer_2: This layer communicates with many groupings of physical sensors and attempts to place them into one classified group. In addition, this layer is the more important layer in our proposed design. The layer allows sensor service providers and other IT resources to be managed remotely without concern for the location of the real sensor sites. This layer can be considered the most important layer in our design, which includes servers, storage and networks devices. In this layer we use open source servers and applications and apply the concept of virtual servers to reduce the total cost of ownership.
3) Layer_3: This layer corresponds with consumers/end users and their applicable requests. Numerous consumers need to contact the valued data sensor from many kinds of operating system platforms using different types of application.

From the above, we can say that we have many types of actor (sensor owner, sensor-cloud administrator and end users) and many components in the cloud sensor (client, e-portal server, provision server and resources manager server, virtual sensor group, monitoring server and physical sensors). This proposes a schema which provides the transparency and scalability for end users to connect physical sensors. Figure 3 shows actors and components in our proposed design.

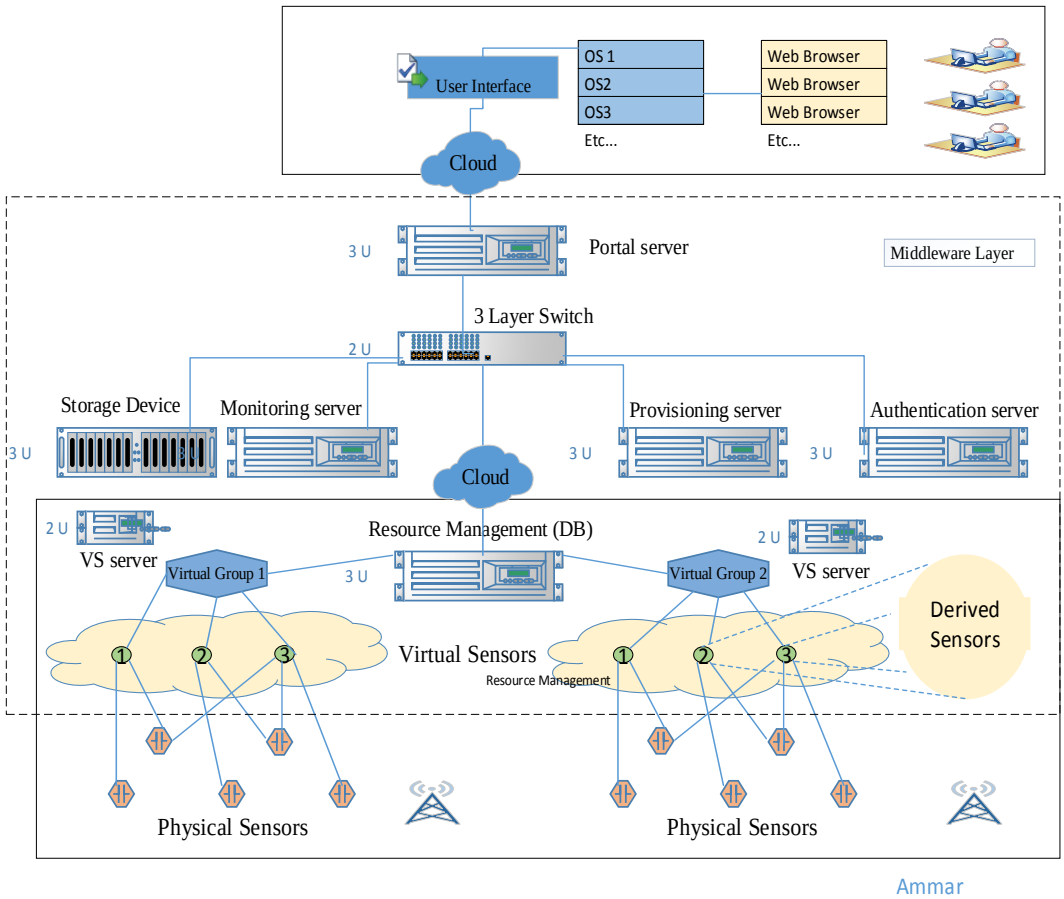

Figure 3. Actors and components in the proposed design

10. Issues in the Sensor Cloud Design

There are many issues regarding the design of sensor clouds. Moreover, there are no modern concepts for applications and implementation from previous proposed structures. Therefore, to come out, there are many issues that should be considered while working with sensor cloud design, which includes but is not limited to cycle, as shown in Figure 4:

Figure 4. Design issues cycle

Sensor networks Security usually have several restrictions similar to other network types. Therefore, it is not logical to implement a conventional security policy such as the traditional security steps, consequently, to build a security operational platform for the sensor cloud, we need first to understand the nature of these restrictions on the form of the network. Some sensor network restrictions are, Unreliable Communication, Limited Resources and Unattended Operations.

11. Pros and Cons of the Proposed Design

Following are some Pros. and Cons. Of our proposed design:

A. Pros

1) Transparency: The consumer does not need to worry about the details.
2) Scalability: The Sensor Cloud offers ease of management to the end consumer.
3) Reliability: The consumer can follow up the status of his own virtual sensors from anywhere.
4) Flexibility: The consumer can rapidly start to use the physical sensors by using virtual sensors remotely.
5) The consumer can make his group of sensors depend in his need by consuming virtual sensor groups.
6) The owner of the physical sensors can track the usage of the sensors.

B. Cons

1) ICT resources need for a sensor-cloud infrastructure should be well configured to serve this design purpose.
2) Each physical sensor needs templates for virtual sensors to be joined.
3) Bandwidth and connectivity types between the consumer and cloud-sensor servermay be a factor of weakness.
4) The possibility of shearing data from some of the physical sensors gives the possibility of loss of precision data in real time.

12. Lab Test

In our lab, we used one Windows Server 2012 and three Red Hat Linux servers to accomplish our proposed design. We also used Oracle Virtual Box as the virtual environment to host all our servers. Each virtual machine had 1 CPU 2.1HZ, Memory 2 GB and HD 15 GB. Our test lab showed high performance and a good total cost of ownership and effective response time figure 6 show our lab workbench. We applied a stress load (100,200,300,350,400) request and each user will run 100 threads simultaneously) to our design and gathered the results of system performance. Tables 1, 2, 3, 4 and 5 show the static results obtained respectively, while table 6 show our system performance compared to online project performance [26].

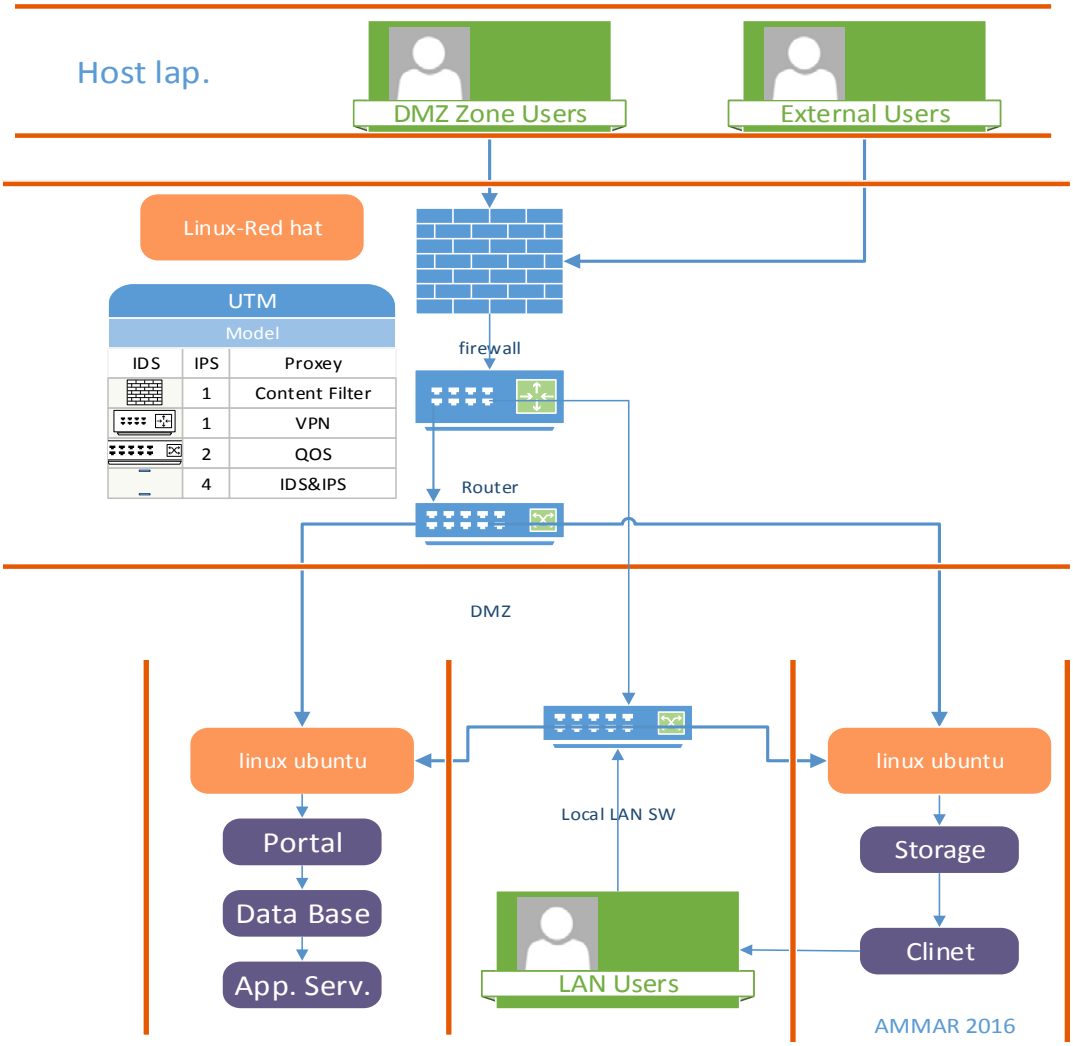

Figure 5. Lab workbench

Table 1. 100 Threads run 100 time

Login Request	100	0.014	15	159	691.66	1.4	110.56	15414
Logout Request	100	0.318	10	100	614.01	0.1	1.54	14
HTTP Request	10000	0.068	5	146	91.6	49.4	1188.81	46489

Table 2. 200 Threads run 100 time

Login Request	200	0.235	9	3203	570.35	3.3	358.58	25323
Logout Request	200	0.033	5	5352	935.55	0.8	0.99	33
HTTP Request	20000	0.273	5	3030	222.53	39.5	2300.93	37389

Table 3. 300 Threads run 100 time

Login Request	300	1.009	7	7186	3.96	0.3	80.81	15313
Logout Request	300	0.106	1	1503	609.18	1	1.6	13
HTTP Request	30000	0.193	6	517	370.66	51.6	1387.78	37389

Table 4. 350 Threads run 100 time

Login Request	350	1.789	5	311	357.7	7.7	513.55	35533.5
Logout Request	350	1.755	51	55	339	7.3	8.15	35
HTTP Request	35000	1.393	5	355	333	55.5	3573.39	57589

Table 5. 400 Threads run 100 time

Login Request	450	1.731	13	7778	1135.83	11.7	388.73	35535
Logout Request	450	1.177	31	3385	788.33	11.7	11.88	1135
HTTP Request	45000	1.513	5	3513	511.55	53.5	3538.7	57588

Table 6. System performance compared to online project performance

Model	On line Project Test			Our system		
Term	Request	Ave.(ms)	Throug.	Request	Ave.(ms)	Throug
Login	30,000	5,100	30.6	400	1.731	11.7
Logout	30,000	22	31.5	400	1.177	11.7
HTTP	N/A	N/A	N/A	40000	1.513	53.5

13. Conclusion

In this paper, we present a sensor cloud structure which enables the virtualization of physical sensors according to on-demand consumers' requirements without worrying about the details of how to implement virtual sensors. Our design provides transparency and flexibility to end users to host their own sensors. Moreover, our results show high system performance when applying the stress load test and the lowest total cost of ownership. On the other hand, using a communication line among the cloud sensor nodes is a formidable task, since the sensor cloud has many issues, such as security and integrity. Addressing these issues and attempting to develop them along with working in developing a new design of virtual environment will contribute to increasing the applications based on this type of sensor cloud architecture. Our proposed design is a big step towards the rapid progress of the new technology term “Internet of Things” which will be implemented in the future.Future work may focus on developing heterogeneous distributed system designs and developing protocols to deal with physical sensors in standard ways, security issues for communication lines and allowing people to contribute to management design and allowing them to be part of the sensor cloud model by using their own sensors.

Acknowledgments

The authors A. J., A. T. and A. R. thank the Iraqi Board of Supreme Audit Iraq/Baghdad and Baghdad University, which contributed effectively to give us this opportunity for publication.

References

[1] Akshay N, Kumar MP, Harish B, Dhanorkar S. An efficient approach for sensor deployments in wireless sensor network*. IEEE Emerging Trends in Robotics and Communication Technologies (INTERACT), International Conference*. 2010: 350 – 355.

[2] Madoka Y, Takayuki K. *Sensor-Cloud Infrastructure - Physical Sensor Management with Virtualized Sensors on Cloud Computing.*I BM Research – Tokyo, 13th International Conference on Network-Based Information Systems. 2010: 1-3.

[3] Thomas F. the Fusion and Integration of Virtual Sensors. *College of William and Mary*. 2002.

[4] Pethuru R. Cloud Enterprise Architecture. *CRC Press*. 2012: 312-320.

[5] Ovidiu V, Peter F. Internet of Things. Global Technological and Societal Trends from Smart Environments and Spaces to Green ICT.*River Publishers.* 2011.

[6] Shashi P, Thomas F, La Porta, Christopher G. *Sensor Network Operations*. John Wiley & Sons. 2006: 104-116.

[7] Sanjay M, Vimal K and Rashmi D. Sensor Cloud: A Cloud of Virtual Sensors*. IEEE next-generation mobile computing*. 2014: 31.

[8] Yuriyama M, Kushida T. Sensor-Cloud Infrastructure: *Physical Sensor Management with Virtualized Sensors on Cloud Computing.* IEEE, Network-Based Information Systems (NBiS), 13th International Conference. 2010: 1 – 8.

[9] Cuno P. Getting Started with the Internet of Things: Connecting Sensors and Microcontrollers to the Cloud". *O'Reilly Media, Inc., ISBN1449393578, 9781449393571,* Ch4. 2011.

[10] Honbo Z. *The Internet of Things in the Cloud*: *A Middleware Perspective*. CRC Press. 2013.

[11] CO Rolim, FL Koch, CB Westphall, J Werner, A Fracalossi, GS Salvador. *A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions.* 2nd Intl Conference on eHealth, Telemedicine, and social medicine. 2010.

[12] Miranda J, Makitalo N, Garcia-Alonso J, Berrocal J, Mikkonen T, Canal C, Murillo and JM. "From the Internet of Things to the Internet of People". *IEEE Journals &Magazines*. 2015; 19(2): 40 – 47.

[13] Guillen J, Miranda J, Berrocal J, Garcia-Alonso J, Murillo JM and Canal C. People as a Service: A Mobile-centric Model for Providing Collective Sociological Profiles. *IEEE Journals & Magazines,* 2014; 31(2): 48 – 53.

[14] Sanjay M, Vimal K and Rashmi D. Sensor Cloud: A Cloud of Virtual Sensors. *IEEE Journals & Magazines*. 2014; 31(2): 70 – 77.

[15] Hoon-Ki L, Jong-Hyun J and Hyeon-Soo K. *Provision of the Social web of Things. Consumer Electronics*. Berlin (ICCE-Berlin). IEEE Fourth International Conference. 2014: 404 – 407.

[16] Roel P. Security Architecture for Things That Think. PhD Thesis Arenberg Doctoral School of Science, Engineering & Technology Faculty of Engineering Department of Electrical Engineering (ESAT). 2012.

[17] Miranda J, Makitalo N, Garcia-Alonso J, Berrocal J, Mikkonen T, Canal C, Murillo and JM. From the Internet of Things to the Internet of People. *IEEE Journals & Magazines*. 2015; 19(2): 40 – 47.

[18] Dominique G and Vlad T. *Towards the web of things: Web mashups for embedded devices*. Second Workshop on Mashups, Enterprise Mashups and Lightweight Composition on the Web (MEM 09). 2009.

[19] Erik W. Putting things to REST. Technical Report UCB iSchool Report 2007-015, School of Information, UC Berkeley. 2007.

[20] Markus W, Adrian M, Thorsten S and Elgar F. *Towards a Power Pedia a Collaborative Energy Encyclopedia.*Workshop of Ubiquitous computing forSustainable Energy (UCSE), at UbiComp, Copenhagen, Denmark. 2010.

[21] Chee-Yee C and Kumar S. *Sensor Networks: Evolution, Opportunities, and Challenges*. Proceedings of the IEEE. 2003; 91(8): 1247-1256.

[22] Manoj K. Wireless Sensor Networks: Security Issues and Challenges. IJCIT, ISSN 2078-5828 (PRINT), ISSN 2218-5224. 2011; 02(01): 110746.

[23] OGC, Sensor Web Enablement (SWE) standards", [Online]. Avalibal: http://www.opengeospatial.org/, [accessed 17 Oct 2015].

[24] Mike B, Alexandre R. OpenGIS Sensor Model Language (SensorML) Implementation Specification. Open Geospatial Consortium, Inc. 2007.

[25] Jih-Wei W, Ding-Wei C, Jehn-Ruey J. *The Virtual Environment of Things (VEoT): A Framework for Integrating Smart Things into Networked Virtual Environments.* Internet of Things (iThings), IEEE International Conference. 2014: 456 – 459.

[26] Simon S. Quick Wins in Liferay Performance: Testing and Tuning Liferay Portals. [Online]. Available: https://www.firelay.com/resources/blog/-/blogs/liferay-performance-testing-and-tuning [Accessed 28 Dec. 2015].
[27] Aws S, Ammar JH, Ihab A and Abdalrazak T. Development and status of vehicular ad hoc networks. *WELFENIA*. 2016; 23(2).