A Secure Cloud-Enabled Wireless Sensor Network Platform

Felix Njeh and Dr. Bo Yang
Department of Computer Science

Bowie State University, Bowie, Maryland 20715

Abstract **-** *Nowadays, Wireless Sensor Networks (WSN) have become a key enabling technology and consequently demands a secure, distributed and globally available network of sensors. Various technologies have evolved and are used to facilitate the deployment and use of WSNs. The rapid development in Micro-Electro-Mechanical Systems (MEMS) technology has facilitated the development of smart and highly capable sensors to solve a multitude of real world problems.*

Keywords: *Wireless Sensor Networks, Cloud Computing, SOA*

1 Introduction

The emergence of the Internet, for example has enabled the deployment of sensor network applications accessible through the World Wide Web. Cloud Computing has become another technology of choice for many due to the numerous benefits it brings to the Information Technology industry. Grid Computing uses the concept of parallel processing to introduce a platform on which a computationally intensive problem could be solved by harnessing the unused compute power of many computer resources distributed globally. The Internet of Things is another paradigm that extends the capabilities and use of WSNs.

With these concepts, we propose a Service-Oriented Architecture (SOA) in which WSNs distributed world-wide can be interconnected into a secure global network of sensors. This secured and unified platform will provide the end-user with a large choice of virtual configurations for sensing, monitoring and analytics capabilities. An experimental testbed has been setup and a feasibility study of the model will be conducted and the results analyzed.

2 Background

2.1. Wireless Sensor Networks

A Wireless Sensor Network (WSN) consists of a large number of low-cost, low-power, multifunctional and resource-constrained sensor nodes with each sensor node consisting of sensing, data processing, and communicating components; these nodes can operate unattended for long durations. Sensor nodes perform measurements of some physical phenomena, collect and process data, communicate with other peers or a central information processing unit, the sink. These nodes are capable of sensing various phenomena, such as Pressure, Temperature, Humidity, Position, Velocity, Acceleration, Force, Vibration, Proximity, Motion, Biochemical agents, and more.

There are several characteristics that influence the design and use of WSNs. Some of such considerations include: robustness, fault tolerance, self-configuration, energy efficiency and lifetime maximization. Standards have been developed to remediate some of the issues in Sensor Networks. A good example is the ZigBee/IEEE 802.15.4 standard.

2.2. ZigBee/IEEE 802.15.4

ZigBee is a specification for a reliable, low-cost, low-power consumption, self-organizing, ad-hoc, mesh networking standard. It is based on the IEEE 802.15.4 standard for Low-Rate Wireless Personal Area Networks. ZigBee operates in unlicensed bands - 2.4 GHz Global Band at 250kbps, 868 MHz European band at 20kbps and 915 MHz North American band at 40kbps. ZigBee was initiated when it became clear that Wi-Fi and Bluetooth technologies were going to be unsuitable for many wireless applications. The standard provides low-cost, long battery life, secure wireless networking for tracking, control and monitoring. Compared to other wireless standards, ZigBee connects the widest variety of devices. With these capabilities, ZigBee can be used for military applications, industrial control, embedded sensing, medical data collection, smoke and intruder warning, building automation, home automation, and more.

Market Name Standard	ZigBee® 802.15.4	--- GSM/GPRS CDMA/1xRTT	Wi-Fi™ 802.11b	Bluetooth™ 802.15.1
Application Focus	Monitoring & Control	Wide Area Voice & Data	Web, Email, Video	Cable Replacement
System Resources	4KB - 32KB	16MB+	1MB+	250KB+
Battery Life (days)	100 - 1,000+	1-7	.5 - 5	1 - 7
Network Size	Unlimited (2^{64})	1	32	7
Maximum Data Rate (KB/s)	20 - 250	64 - 128+	11,000+	720
Transmission Range (meters)	1 - 100+	1,000+	1 - 100	1 - 10+
Success Metrics	Reliability, Power, Cost	Reach, Quality	Speed, Flexibility	Cost, Convenience

Table 1.0: Comparison of ZigBee and other wireless standards
Source: http://www.zigbee.org/About/FAQ.aspx

The IEEE 802.15.4 standard provides specifications for point-to-point or point-to-multipoint networks. The nodes in the network are either full function devices or reduced function devices.

WSNs have been studied for a good length of time resulting in improved sensors or sensor-enabled systems. These WSNs have evolved and have become quite popular that they spand various applications and industries. WSNs have been used in health, commercial, military applications including battle-field surveillance and enemy tracking, home automation and security, habitat and environmental monitoring. This illustrates the significance of WSNs in these industries.

2.3. Cloud Computing

Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models [2]. Figure 1 below illustrates the service and deployment models.

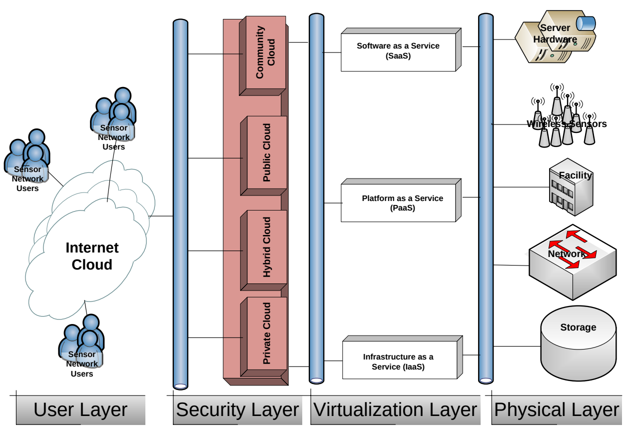

Figure 1: The integrated Cloud WSN Platform

Cloud Computing consists of three service models, Software as a Service (SaaS), Platform as a service (PaaS), and Infrastructure as a Service (IaaS); and four deployment models, Private cloud, Hybrid cloud, Public cloud and Community cloud.

Service Models

The three service models include Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

2.3.1. Software as a Service (SaaS)

This is a software delivery model in which the provider gives customers on-demand access to the applications hosted in a cloud infrastructure. The infrastructure is managed by the provider while the consumer has only limited user-specific application configuration settings. SaaS is increasingly becoming a common delivery model for most business applications. The consumer usually pays a subscription fee instead of a licensing fee.

2.3.2. Platform as a service (PaaS)

This service delivery model allows the customer to rent the cloud infrastructure (virtualized servers and associated services) to run consumer-created or acquired applications or to develop and test new ones. The infrastructure is managed and controlled by the provider; the consumer has some control over the deployed applications and possibly application hosting environment configurations.

2.3.3. Infrastructure as a Service (IaaS)

IaaS is a delivery capability in which the consumer provisions processing, storage, networks, and other fundamental computing resources. The consumer can deploy and run arbitrary software (operating systems and applications) but does not manage or control the underlying cloud infrastructure.

Deployment Models

The deployment models include Private cloud, Hybrid cloud, Public cloud and Community cloud.

2.3.4. Private Cloud

With this model, the internal or corporate cloud infrastructure (systems and services) is operated solely for an organization. This gives the organization better management and control over their data and systems. It is also considered a proprietary network or a data center that supplies hosted services to a limited number of people.

2.3.5. Hybrid Cloud

A Hybrid Cloud is made up of at least one private cloud and at least one public cloud. An example is when a vendor has a private cloud and forms a partnership with a public cloud provider, or a public cloud provider forms a partnership with a vendor that provides private cloud platforms. In other instances, the organization owns and manages some of the cloud resources internally while others are made available externally. A hybrid cloud provides the consumer the best of both worlds.

2.3.6. Public Cloud

A public cloud is a cloud model in which the cloud provider makes the cloud infrastructure available to the general public; and is owned by the cloud provider. This model is also considered as external cloud. It has several advantages to include: lower cost of deployment, scalability and efficient use of resources (since you only pay for what you use).

2.3.7. Community Cloud

A Community Cloud allows the cloud infrastructure to be shared by several organizations and supports a specific community that has shared concerns. This model can be managed by the organizations involved or a third party, and may exist on premise or off premise.

3 Related Works

In (Briefings, 2009), the authors evaluated the potentials of the integration of Wireless Sensor Networks and Cloud Computing and drew the conclusion that this marriage is not only possible but makes it more feasible to collect, analyze and share sensor data. A content-based publish/subscribe platform is proposed; where the WSNs publish the data collected while the subscribers consume the data. Services are delivered to consumers continuously, periodically, event-based or query-based.

(Hassan & Korea, 2009) propose “a content-based pub-sub model which simplifies the integration of sensor network with cloud based community centric applications”. In this study, the provider also publishes data and consumers access the data and applications through a cloud infrastructure on-demand from anywhere. A Pub/Sub broker monitors, processes and delivers events to registered users through SaaS applications. An event matching algorithm matches subscribed users to events of interest. A simulation was done to test this algorithm but with no use of any real-world data. The literature does not clearly state how data transitions through the different layers or stacks of the CC model.

WSNs generate huge amounts of data. (Bose & Liu, n.d.) believe that sensor data will continue to increase exponentially, with the side effect that traditional platforms cannot sustain this increase. They suggest that CC is a viable answer to this problem. (Kurschl & Beer, 2009) also identify the massive amounts of data generated by WSNs as one of the key motivations to amalgamate sensor networks with CC, and agree that with other studies that the resulting platform will provide for interoperability with other vendors’ sensors, scalability of system resources (storage, compute, network, etc.), accessibility to sensor data from any location worldwide. A model is proposed that is based on pipes and filters; where the filters process and transform input data while pipes provide an interconnection mechanism for filters. Base services identified include: Sensor Data Management, Runtime for Filter Chains, Filter Chain and Filter Management, Visualization, and Notification Service. A prototype Energy Monitoring shows a Zigbee based WSN for gathering energy consumption data and dispatching into the Cloud.

(Benson, Dowsley, & Shacham, 2011) examines the issue of geolocation of data in the Cloud and propose a method of efficiently retrieving data stored as multiple copies in geographically disparate datacenter locations. For critical sensor applications, it is important to know the location of data in the Cloud to ensure accessibility and security. It is important to route application requests to the nearest data center in order to minimize response time.

In (Hauswirth & Decker, 2007), the authors discuss the unification of the real and the virtual worlds using sensor technologies and the Semantic Web; with applications in monitoring, manufacturing, health, tracking and planning. (Melchor, n.d.) proposes a toolkit for sensor-cloud integration. Both approaches fail to identify or leverage the features of CC as enabling characteristics.

4 Motivation

Sensor networks are found in disparate locations all around the world supporting a myriad of applications. For example, in military applications we find robots carrying sensors in remote tactical environments to monitor or track the enemies.

With the recent advancements in cloud computing, we realized the importance of defining a standard architecture that unifies these disparate wireless sensor networks. This will provide for global connectivity and accessibility to these sensor networks. Figure 1 below illustrates sensor networks in disparate locations around the world. In Figure 3, we illustrate the experimental network setup showing a WSN connecting to the iDigi Cloud from which web client applications provide sensor data or information to approved and authenticated users.

5 The Integrated Cloud WSN Platform

Figure 1 shows the integration between the Cloud and Wireless Sensor Networks. WSNs are often omitted as part of the Cloud infrastructure. In this paper we strive to fit WSNs into the Cloud architecture and conduct research to find out how well the WSNs fit with other famous IaaS components. In order to perform these findings, we look at performance metrics of worldwide Cloud providers to gauge if the existing platform gives room for the introduction of other infrastructure components.

Our goal is to leverage the beneficial features of Cloud Computing which include on-demand self-service, broad network access, resource pooling (location independence), rapid elasticity, measured service, massive scale, homogeneity, virtualization, resilient computing, geographic distribution, service orientation and advanced security technologies.

5.1. Cloud Performance Metrics

Performance and availability are key metrics when considering any Cloud application. CloudSleuth[1] provides us with the tools to measure these metrics. From the available data we see that Cloud providers in the United States and Europe provide reasonable response time of less than 3 seconds (see Figure 2a below).

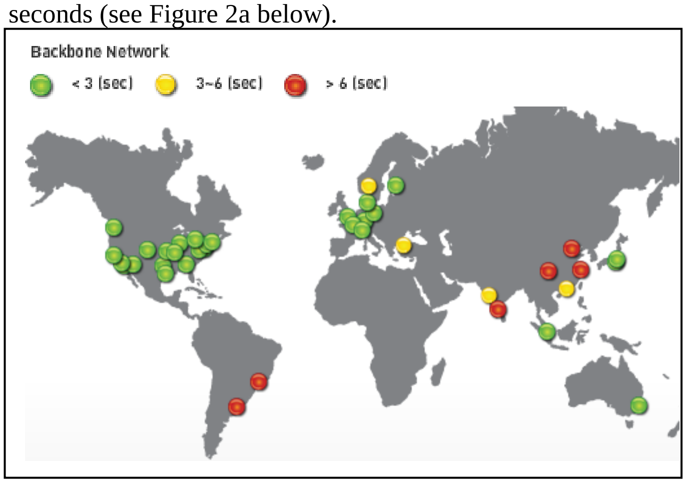

Figure 2a: Performance of worldwide Cloud Providers Source: https://cloudsleuth.net

Figure 2b: Performance of worldwide Cloud Providers Source: https://cloudsleuth.net

In terms of availability, most of the major cloud service providers worldwide were available almost 100% of the time, this is quite promising and gives us confidence that our integrated platform will survive in real applications.

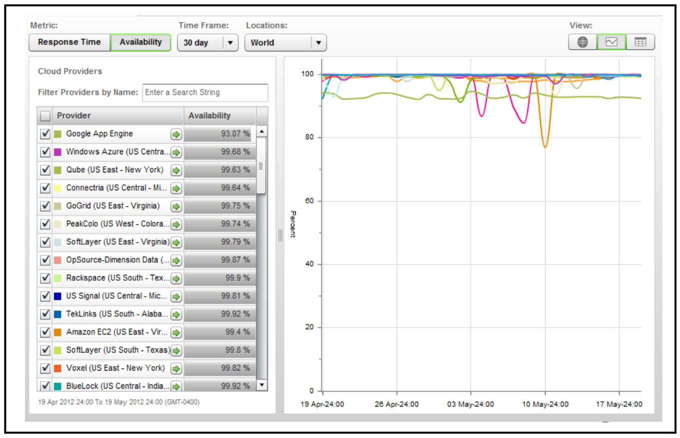

Figure 2c: Performance of worldwide Cloud Providers Source: https://cloudsleuth.net

6 Experimental Setup

In our experiment, we setup a WSN that monitors light, temperature, power draw, and control. The WSN connects to a Digi[2] gateway which sends all traffic into the iDigi cloud through an access gateway.

The setup uses the iDigi[3] Gateway Development platform which consists of the Digi ConnectPort® X4 (ZigBee Ethernet gateway), the XBee Smart Plug™, the XBee Sensor and the ESP Integrated Development Environment (IDE) for iDigi Dia/Python development. The setup provides tools to setup a ZigBee network, design, test and upload applications, make web service calls and provide connectivity to the Internet. Web applications can be designed to access real-time sensor data. The experimental testbed is illustrated below.

Figure 3: iDigi Gateway Development kit Source: http://www.digi.com/

[1] *https://cloudsleuth.net*

[2] Digi International Inc. develops networking products and solutions.

[3] http://www.digi.com/

This platform is called the iDigi Device Cloud. It facilitates the creation and deployment of device applications. This iDigi Cloud platform provides desirable features such as performance, reliability, scalability, security, seamless device and application integration.

6.1. Data Collection and Visualization

In our prototype, the wireless sensors collect data which is retrieved and transmitted wirelessly through the XBee network. The portable battery-powered sensors can be dropped into an environment of interest for data collection and communication.

The information collected is displayed as a dashboard, graphs or charts. Data or information collected is displayed through a web interface or on a smart device.

- **Light** - the XBee Smart Plug Ambient light sensor measures indoor light intensity.
- **Temperature** - the XBee Sensor is a battery-powered sensor that measures temperature and light.
- **Power draw** - the XBee Smart Plug detects current draw from the AC socket (standard AC 110V, 3-prong).
- **Control** – The XBee Smart Plug provides power control to the user outlet. It is configured through the XBee module's digital I/O channel, D4 which can be set to high or low to turn power on or off.

Our experimental setup was limited to one sensor network. For that reason we extrapolate the capability of the experiment by looking at the behavior of the worldwide cloud content delivery network (CDN). Figures 2a Figure 2b and Figure 2c above show availability and response time for worldwide cloud providers.

7 Conclusions

In this paper we propose a new type of platform which integrates and leverages the features of two key technologies, Cloud Computing and Wireless Sensor Network. This unified platform leverages the key benefits of two core technologies to provide a secure platform through which sensor data can be processed and assimilated. We ran Cloud performance tests for availability and response time to weigh Cloud performance through worldwide Cloud providers' backbones. The performance results indicate the potentials of Cloud Computing and further give us confidence in our endeavor to merge the two technologies together to provide a secure worldwide cloud-enabled WSN services.

In future works, we will address the lack of widely accepted open standards and interoperability between sensor-cloud platforms. Data analytics and security also require more research to highlight issues affecting the platform.

8 References

[1] Peter Mell, Tim Grance. "Effectively and Securely Using the Cloud Computing Paradigm", NIST, Information Technology Laboratory.

[2] NIST Cloud Computing Standards Roadmap. "NIST CCSRWG – 070 Eleventh Working Draft". May 2, 2011

[3] iDigi® Gateway Development Kit. " Development Kit for ZigBee Gateways and iDigi Platform"

[4] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal: "Wireless sensor network survey. Computer Networks" 52(12): 2292-2330 (2008)

[5] The ZigBee Alliance, http://www.zigbee.org/About/AboutTechnology/Standards.aspx, 2011 ZigBee Alliance

[6] Theoretical and practical aspects of military wireless sensor networks"

[7] Madoka Yuriyama, Takayuki Kushida, "Sensor-Cloud Infrastructure - Physical Sensor Management with Virtualized Sensors on Cloud Computing", IBM Research - Tokyo, March 17, 2010

[8] Peter Mell and Tim Grance. "The NIST Definition of Cloud Computing". 10-7-09

[9] Duane Nickul et al. "Service Oriented Architecture (SOA) and Specialized Messaging Patterns"

[10] Peter Mell, Tim Grance. "The NIST Definition of Cloud Computing. NIST Special Publication 800-145

[11] Mark Gaynor, Steve Moulton et al. "Integrating Wireless Sensor Networks with the Grid", AUGUST 2004

[12] Cuno Pfister. "Getting Started with the Internet of Things". 2011. Published by O'Reilly Media, Inc.

[13] Aditya Goel and Ajaii Sharma. "Performance Analysis of Mobile Ad-hoc Network Using AODV Protocol". International Journal of Computer Science and Security (IJCSS)

[14] Briefings, S. (2009). Can We Plug Wireless Sensor Network to Cloud? cloud computing pinnacle of IT Infrastructure democratization, 7(7), 33. Retrieved from http://www.infosys.com/infosys-labs/publications/documents/cloud-computing.pdf#page=35

[15] Hassan, M. M., & Korea, S. (2009). A Framework of Sensor - Cloud Integration Opportunities and Challenges, 618-626.

[16] Kurschl, W., & Beer, W. (2009). Combining cloud computing and wireless sensor networks. Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services - iiWAS '09, 512. New York, New York, USA: ACM Press. doi:10.1145/1806338.1806435

[17] Bose, B. S., & Liu, R. (n.d.). Cloud Computing Complements Wireless Sensor Networks to, 10-11.

[18] Kang, Y., Zhou, Y., Zheng, Z., & Lyu, M. R. (2011). A User Experience-Based Cloud Service Redeployment Mechanism. 2011 IEEE 4th International Conference on Cloud Computing, 227-234. Ieee. doi:10.1109/CLOUD.2011.20

[19] Benson, K., Dowsley, R., & Shacham, H. (2011). Do you know where your cloud files are? Proceedings of the 3rd ACM workshop on Cloud computing security workshop - CCSW '11, 73. New York, New York, USA: ACM Press. doi:10.1145/2046660.2046677
[20] Hauswirth, M., & Decker, S. (2007). Semantic Reality – Connecting the Real and the Virtual World Position Paper, 1-4.