Hindawi Publishing Corporation
Scientific Programming
Volume 2016, Article ID 5083074, 12 pages
http://dx.doi.org/10.1155/2016/5083074

Research Article

Monitoring Dangerous Goods in Container Yard Using the Internet of Things

Lianhong Ding, Yifan Chen, and Juntao Li

School of Information, Beijing Wuzi University, Beijing, China

Correspondence should be addressed to Lianhong Ding; lhdingbwu@sina.com

Received 6 August 2016; Revised 30 October 2016; Accepted 16 November 2016

Academic Editor: Xiong Luo

The Internet of Things (IoT), a network of objects, has been regarded as the next revolution for the global information industry after the Internet. With IoT, many intelligent applications can be accomplished or improved. This paper presents a framework for dangerous goods management in container yard using IoT technology. The framework consists of three layers: perceptual layer, transport layer, and application layer. It offers an infrastructure for management and data analysis and utilization. According to the features of dangerous goods, the framework can be enhanced for container information forecast, container gate-in and gate-out management, environment parameters monitoring, and fire control as well. In order to verify our method, a prototype system is developed, which shows good performance. With our method, safe operation of dangerous goods in container yard can be accomplished.

1. Introduction

The Internet of Things (IoT) is an emerging global Internet-based information architecture facilitating the exchange of goods and services in global supply chain networks [1]. IoT was first proposed in 1999 by Auto-ID Center [2]. The concept of IoT was widely accepted after a report from ITU released in 2005 [3]. The growth of IoT community has been encouraged by the rapid development of wireless sensor and actuator networks, identification tags such as barcode and RFID (Radio Frequency Identification), and electronic prototyping platforms such as Arduino [4].

IoT technology has been widely adopted in various fields, such as intelligent transportation and environmental protection. With the acceleration of the world economic integration, container transportation has become the most important transport mode for the world trade. Container yard is the container storage buffer in the whole operation chain for a port. The efficient and safe operation of the container yard will increase the port's relative capacity, thus improving the operation efficiency of the port. Regarding the importance of security, container yard is usually divided into two areas: the storage area for general goods and storage area for dangerous goods.

The logistics system of dangerous goods mainly consists of two parts: transportation and storage. At present, dangerous goods are mainly transported through the sea or road. The safety precautions and insurance policy for the shipping process are rather mature. Thus, dangerous goods can be protected well during their transportation. Therefore, the management and control in the storage process, especially in container yard, should be paid more attention.

A large proportion of serious accidents are caused by dangerous materials. A huge explosion happened in a container yard operated by a logistics company called Rui Hai International Logistics Co. Ltd. on 12 August 2015 in Tianjin, China. The Tianjin explosions were a series of explosions that killed over one hundred people and injured hundreds of others [5]. Rui Hai handles hazardous chemicals within the Port of Tianjin. In addition to the vast quantities of sodium cyanide and calcium carbide, 800 tons of ammonium nitrate and 500 tons of potassium nitrate were at the blast site [6]. A fire department spokesman confirmed that the firefighters had used water in combating the initial fire, which may have led to water being sprayed on calcium carbide, releasing the highly volatile gas acetylene. This may have detonated the ammonium nitrate [7]. The direct cause for this accident is that the nitrocellulose in containers spontaneously combusts and explodes due to high temperature. This brings about the burning of the nitrocellulose and other hazardous chemicals in the adjacent containers and leads to the explosion of ammonium nitrate and other hazardous chemicals stacked in the yard [8].

To avoid similar accident, the monitoring of dangerous materials in container yard should be paid more attention. Obviously, IoT is a good solution for the monitoring system. This paper proposes a framework to manage dangerous goods in container yard. With the support of IoT, the framework helps operators obtain information about different dangerous materials, such as firefighting knowledge and temperature limitation. When emergency occurs, this system can provide related information to the firefighter. It will help the firefighters to use the right method to deal with emergencies, such as burning or explosion. With the help of wireless sensor networks, this system can also provide appropriate management strategies for relevant staffs through temperature monitoring. These strategies are generated according to the current temperature and the storage rules for dangerous materials. Similar directions can be given out according to the environment parameters such as humidity and CO_2 concentrations.

2. The Internet of Things

IoT is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. The basic idea of IoT is the pervasive presence around us of a variety of things or objects. IoT involves many technologies including architecture, sensor/identification, coding, transmission, data processing, network, and discovery [9]. The standard, reliability, and robustness are also key concerns for IoT development.

With the changes of application requirements and the development of technologies, the concept of IoT is developed further [10, 11]. Different IoT definitions have been put forward from different perspectives such as CASAGRAS [12], CERP-IoT [13, 14], and Smart Planet [15]. Thiesse et al. found solutions based on RIFD technology or EPC mechanism [16]. Broll et al. proposed the Pervasive Service Interaction with things [17] and Vazquez et al. showed an integration solution between mobile services and smart objects [18]. Most researches focused on specific application or special function [19] such as security [20, 21], data mining model [22], and network management [23] for IoT. The Future Internet Assembly has been founded by the European Commission to support fundamental and systematic innovation in Europe for realization of the Future Internet [24].

2.1. Architecture of IoT. As a representative of the earlier scheme for IoT, EPC (Electronic Product Code) system is a vision world where all physical objects can be connected by RFID transponder through a global unique EPC code carried by the RFID tag [25]. Networked Auto-ID is an architecture proposed by the MIT AUTO-ID Center. Its target is to connect all objects by sensing devices (such as RFID and bar code) and the Internet. Corresponding architecture consists of physical tag (such as magnetic stripe encoding, barcode, two-dimensional code, and RFID), reader (such as magnetic stripe card reader, barcode reader, two-dimensional code reader, and RFID reader), network (the Internet or Intranet), object name service, and PML (Physical Markup Language) servers [26]. Japan also proposed its IoT prototype, uID IoT. It identifies real-world entities via RFIDs or barcodes, determines context information such as environment parameters from networked sensors, and adapts information services according to the data it obtains. The difference between Networked Auto-ID and uID IoT is that uID IoT collects context information such as environment parameters [27].

2.2. Technologies in IoT. IoT has several different implementation methods, such as RFID, GPS, laser sensor, infrared sensor, and other equipment. In this network, things can interact with each other without human's participation. In fact, the goal of IoT is to realize the automatic recognition and information sharing among things (or goods) through the Internet. Other associated technologies include network, database, and middleware.

RFID is a popular method to fulfill IoT. IoT can utilize RFID wireless communication to build a network of things [28]. RFID makes things "speak." The RFID tag stores rules and information [29]. There is a center system to collect the data from things through the wireless network. It recognizes objects and shares the information based on opening platform. Things can be managed by the center system.

Wireless sensor network is another key technology. Different kinds of sensors can collect context parameters according to application requirement. Generally, these parameters are transmitted by a wireless network such as GPRS. GPS technology and indoor location technique are often adopted by IoT as well.

3. Dangerous Goods Briefing

Dangerous goods are items or substances that may cause a risk to health, safety, property, or the public environment.

3.1. Classification and Identification of Dangerous Goods. The International Maritime Dangerous Goods (IMDG) code was developed as a uniform international code for the transport of dangerous goods by sea covering such matters as packing, container traffic, and stowage, with particular reference to the segregation of incompatible substances. Dangerous goods are classified into different classes according to IMDG code. General provisions for each class or division are given. Individual dangerous goods are listed in the Dangerous Goods List, with the class and any specific requirements.

In general, dangerous goods are classified into 9 classes. Each class is expressed by a single number, such as "class 1." The nine classes of dangerous goods are as follows: class 1, explosives; class 2, compressed gases and liquefied gases; class 3, flammable liquids; class 4, flammable solids; class 5, oxidizing substances and organic peroxide; class 6, toxic and

Table 1: General segregation requirements for hazardous materials.

Class	1.1, 1.2, 1.5	1.3, 1.6	1.4	2.1	2.2	2.3	3	4.1	4.2	4.3	5.1	5.2	6.1	6.2	7	8	9
Explosives 1.1, 1.2, 1.5	*	*	*	4	2	2	4	4	4	4	4	4	2	4	2	4	×
Explosives 1.3, 1.6	*	*	*	4	2	2	4	3	3	4	4	4	2	4	2	4	×
Explosives 1.4	*	*	*	2	1	1	2	2	2	2	2	2	×	4	2	2	×
Flammable gases 2.1	4	4	2	×	×	×	2	1	2	×	2	2	×	4	2	1	×
Nontoxic, nonflammable gases 2.2	2	2	1	×	×	×	1	×	1	×	×	1	×	2	1	×	×
Poisonous gases 2.3	2	2	1	×	×	×	2	×	2	×	×	2	×	2	1	×	×
Flammable liquids 3	4	4	2	2	1	2	×	×	2	1	2	2	×	3	2	×	×
Flammable solids 4.1	4	3	2	1	×	×	×	×	1	×	1	2	×	3	2	1	×
Spontaneously combustible substances 4.2	4	4	3	2	2	1	2	2	1	×	1	2	2	1	3	2	1
Substances which are dangerous when wet 4.3	4	4	2	×	×	×	1	×	1	×	2	2	×	2	2	1	×
Oxidizing substances 5.1	4	4	2	2	×	×	2	1	2	2	×	2	1	3	1	2	×
Organic peroxides 5.2	4	4	2	2	1	2	2	2	2	2	2	×	1	3	2	2	×
Poisons 6.1	2	2	×	×	×	×	×	×	1	×	1	1	×	1	×	×	×
Infectious substances 6.2	4	4	4	4	2	2	3	3	3	2	3	3	1	×	3	3	×
Radioactive materials 7	2	2	2	2	1	1	2	2	2	2	1	2	×	3	×	2	×
Corrosives 8	4	2	2	1	×	×	×	1	1	1	2	2	×	3	2	×	×
Miscellaneous dangerous substances 9	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×

infectious substances; class 7, radioactive materials; class 8, corrosives; and class 9, miscellaneous dangerous substances.

Some classes, classes 1, 2, 4, 5, and 6, are subdivided into divisions. Divisions are expressed by 2 numbers. The first number identifies the class number and the second identifies the variation within that class. For example, oxidizer is class 5, division 1, which should read "division 5.1." The order in which the classes are numbered is for convenience and does not imply a relative degree of danger (i.e., class 1 is not necessarily more dangerous than class 2 or 3).

3.2. Introduction of Dangerous Goods Regulation. There are different demands for different kinds of dangerous materials. The Department of Transportation (DOT) has designated criteria in 49CFR: Title 49—Transportation, Code of Federal Regulations, Hazardous Materials Regulations (HMR), for determining what is considered hazardous for transportation. Definitions of hazardous material designations are included in 49CFR173 and DOT Hazardous Materials Table 49CFR172.101 provides descriptions required for shipping. Here, several rules are considered in our monitoring system:

(1) During the high temperature period (from June 20 to September 10 each year) from 10 a.m. to 4 p.m., it is prohibited to transport divisions 2.2, 3.1, 3.2, 4.2, 4.3, and 5.1.

(2) In the high temperature season, when the temperature exceeds 30 degrees Celsius, the dangerous goods container for spraying should be sprayed every 2 hours.

(3) According to JT 397-2007: the safety rules for handling dangerous cargo container in port, classes 1, 2, and 7 should be directly lifted down.

(4) Different kinds of dangerous goods should be stacked in different areas. Some of them should be maintained within a certain distance. The detailed requirements are given in Table 1. Numbers and symbols in Table 1 are related to the following terms:

(i) 1, away from: effectively segregated so that the incompatible materials cannot interact dangerously in the event of an accident but may be carried in the same compartment or hold or on deck provided that minimum horizontal separation of 3 m (10 feet) projected vertically is obtained.

(ii) 2, separated from: in different compartments or holds when stowed under deck. If the intervening deck is resistant to fire and liquid, vertical separation (i.e., in different compartments) is acceptable as equivalent to this segregation. For "on-deck" stowage, this segregation means separation by a distance of at least 6 m (20 feet) horizontally.

(iii) 3, separated by a complete compartment or hold from: either vertical or horizontal separation. If the intervening decks are not resistant to fire and liquid, then only longitudinal separation (i.e., by an intervening complete compartment or hold) is acceptable. For "on-deck" stowage, this segregation means separation by a distance of at least 12 m (39 feet) horizontally. The same distance must be applied if one package is stowed “on deck” and the other one in an upper compartment.

(iv) 4, separated longitudinally by an intervening complete compartment or hold from: vertical separation alone does not meet this requirement. Between a package “under deck” and one “on deck,” a minimum distance of 24 m (79 feet) including a complete compartment must be maintained longitudinally. For “on-deck” stowage, this segregation means separation by a distance of at least 24 m (79 feet) longitudinally.

(v) ╳, the segregation, if any, is shown in detail in table of materials.

(vi) ∗, segregation among different class 1 (explosive) materials is governed by the compatibility table.

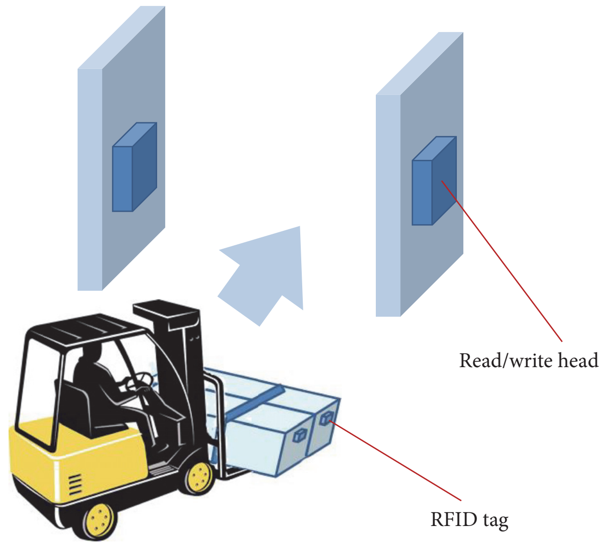

Figure 1: Gate-in and gate-out procedure with RFID.

4. Monitoring System for Dangerous Goods Using IoT

4.1. Requirement Analysis. Considering the regulations for dangerous materials introduced in Section 3.2, the monitoring system should have the following functions:

(1) *Container Information Forecast.* Owners can notice the yard and the information of arriving container in advance through the Internet or other channels. This kind of information can be container number, arrival time, source and destination, and other related information. The management systems can make work plan according to the information.

(2) *Gate-In and Gate-Out Management.* As shown in Figure 1, in the container yard entrance and exit, the reader equipment can get the container information by RFID tag on the container and upload the related information to the system database. The management system automatically records the gate-in information or gate-out information and updates the database in real time.

(3) *Environment Parameters Monitor.* This can be realized by a temperature sensor installed in the container yard. Furthermore, if sensors are deployed within containers, internal environment parameters of the container can be monitored. Different dangerous materials have different ignition points and explosive limits. Sensors inside containers make specific context-aware information for different dangerous materials possible. To a certain extent, this function depends on the deployment of the wireless sensor network. It will be introduced in Section 4.6.

(4) *Firefighting Auxiliary Function.* Firefighting methods for different dangerous materials may be different. For example, if there is a fire of sodium azide, water, foam, and carbon dioxide can be used but sand pressure cannot be used. In order to get right firefighting knowledge for different dangerous materials, two situations should be discussed. First, if the RFID tag on the container still works, the firefighter can get main information about the dangerous goods packaged in the container, including advice about firefighting, by a handhold reader directly. Second, if the tag has been destroyed, fire alert can still be obtained through the container’s position information indirectly. The details will be introduced in Section 4.5.

4.2. System Architecture. In order to support the above functions, we put forward the following architecture for the monitoring system using IoT. The architecture consists of three layers, shown in Figure 2. The first layer is perceptual layer. The task of the perceptual layer is to identify physical object and collect context such as humidity and position. This layer includes RFID tag, RFID reader, sensors, GPS receivers, and handhold terminal. The second layer is transport layer. It transports information by the Internet, Intranet, or wireless network such as GPRS. The object resolution server and container yard monitoring server for dangerous goods form the third layer. The third layer can be regarded as an application layer. The object resolution server identifies the entity by the unique code and finds out the monitoring services related to the object. Container yard monitoring server gives specific context-aware information based on the information provided by object resolution server and with reference to the service rule database.

Unique code tag only records a unique code. All information about objects and position is maintained by object resolution server and container yard monitoring server. By separating the unique code and information, users can easily acquire the latest information on an entity, update that information, and obtain information on other entities related to that entity.

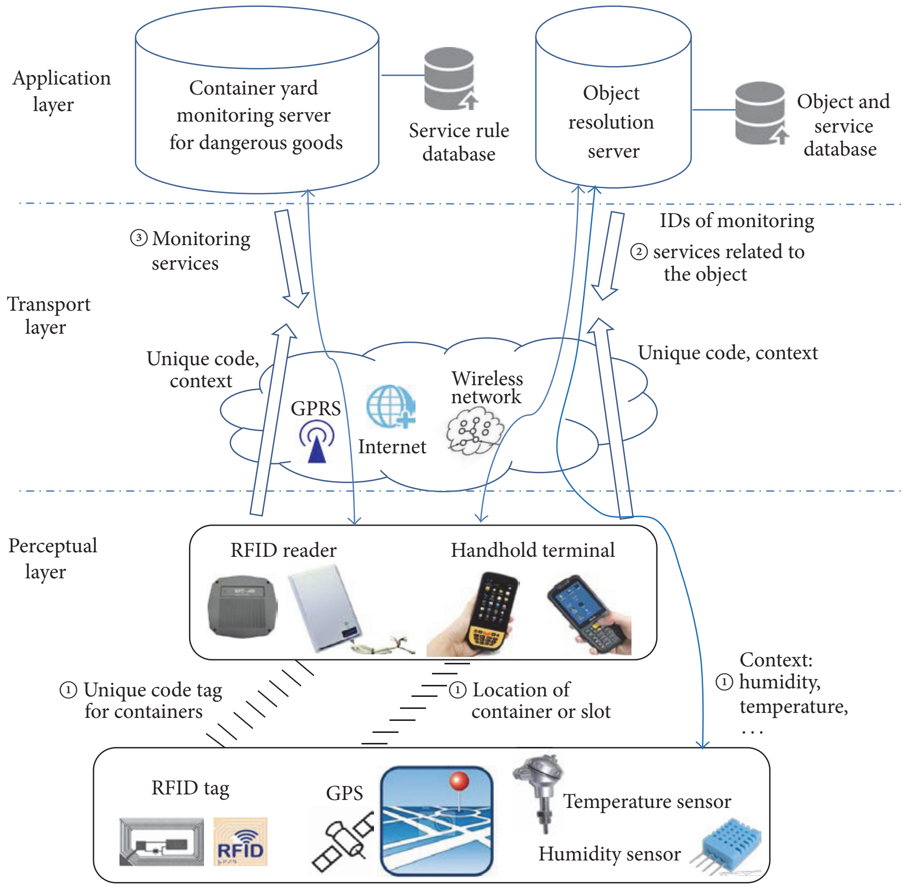

Figure 2: Architecture of the monitoring system for dangerous goods in container yard.

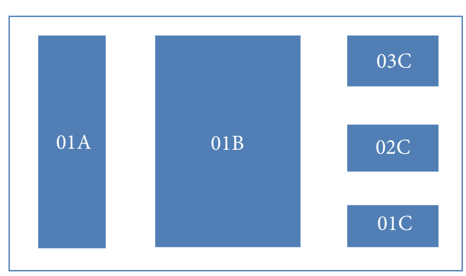

Figure 3: Exemplary layout of the container yard.

The numbers in Figure 2 indicate the order in which the information is processed:

① Obtain unique code of container from RFID tags on container by RFID reader (handhold terminal or reader head on entrance) or location information about container by handhold terminal of GPS. In this step, contexts such as humidity and temperature in containers are collected through sensors and wireless network.

② Object resolution server retrieves the context information about the object identified by unique code and the monitoring services related to object. Here, object and service database records the related information. This kind of information includes the class code of the dangerous materials in the container, the transport rule, and the ID of monitoring services related.

③ When container yard monitoring server receives monitoring service ID, it sends context-aware information about the object (such as container or dangerous goods) back to operators through handhold terminals. The details for the context-aware information are stored in the service rule database.

4.3. Layout of Container Yard and the Encoding Method for Slot Number. Figure 3 shows the overall layout of the container yard for dangerous goods. Different blocks are arranged

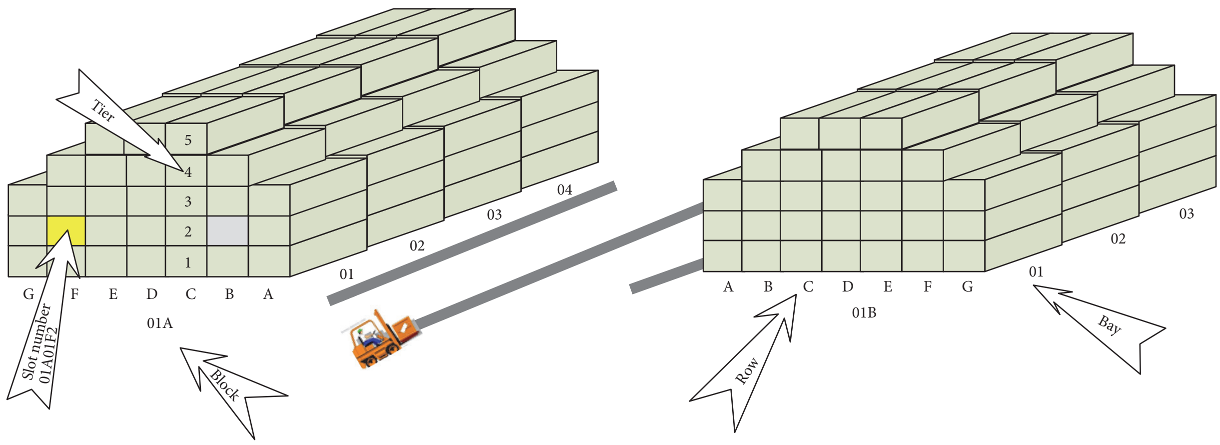

FIGURE 4: Layout of the container yard and slot number.

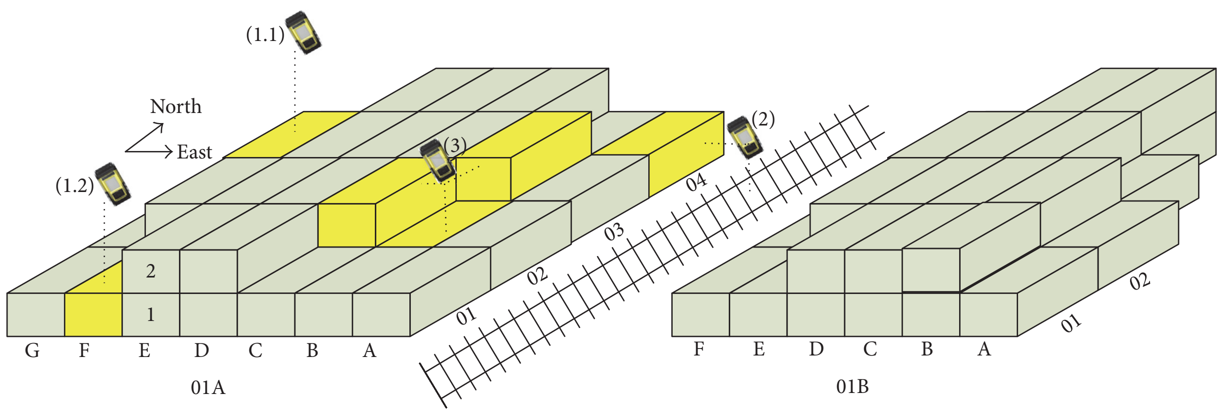

FIGURE 5: Identification of slot by location information.

in the rows and columns. Each block is distinguished by two numbers and one letter. Two numbers indicate the order of a block in the yard from the west to the east. The letter specifies the block order from the south to the north. According to the regulations in the recommendations on the transport of dangerous goods, different kinds of dangerous goods should be stacked in different blocks [30].

Figure 4 is an exemplary layout of a container storage facility, at either seaport terminal, rail intermodal terminal, or inland storage terminal. It illustrates the three-dimensional characteristics of the storage locations at a container yard. Each individual cube represents a container storage location, called slot, where a container can reside. Slot number is used to uniquely identify each slot in the container storage facility. Figure 4 shows a typical slot number, which uses terms such as bay, row, and tier following the block number. A bay value and a row value are used to uniquely identify a container storage location's planetary position in a block. Each bay has the width of one container's length and each row has the width of one container's depth. Containers can also be stacked on top of one another, and the height of the container storage location is represented by a tier value.

In Figure 4, the height is shown and the container cell on the second tier of location (Block 01A, Bay 01, Row F) is uniquely identified by (Block 01A, Bay 01, Row F, Tier 2). So, the slot number is 01A01F2. Such a cell-naming convention allows quick and easy identification of a storage location for containers as well as numerous other types of inventory. Other naming conventions can also be used, and they all reflect uniformity throughout the storage facility in representing the 3-dimensional storage cell locations.

4.4. Gate-In and Gate-Out Operation. As illustrated in Figure 5, each container owns a unique number written in its RFID tag. The container number follows the ISO 6346(1995): freight containers coding identification and marking. It provides a system for general application for the identification and presentation of information about freight containers. It specifies an identification system with mandatory marks for visual interpretation and optional features for automatic identification and electronic data interchange and a coding system for data on container size and type. The class number introduced in Section 3.1 is stored in the tag as well.

Container yard supporting facilities include straddle carriers, shore crane, tire gantry stackers, and forklifts (or stacker). The storage height for dangerous goods container is generally no more than 2 tiers and safety distance should be maintained between different types of dangerous goods containers [30]. These regulations make tire gantry stacker unable to fully play its advantage. At the same time, the flameproof transformation for tire gantry stackers is expensive. Forklift truck for freight containers is more suitable for container yard of dangerous goods.

As shown in Figure 1, RFID read/write heads are mounted on the entrance and exit of the container yard. When a forklift truck, carrying a container, passes through the entrance, the read/write head reads the information from the tag on the container and updates the related information in the object and service database. Similar operations are also performed when a forklift truck passes through the exit.

The electronic tag in RFID system can be active or passive according to whether it has a built-in power supply. Passive RFID tags are used for applications such as access control, file tracking, supply chain management, and smart labels. The lower price makes employing passive RFID systems economical for many enterprises. Passive tags are adopted in our system as well.

Various frequency bands can be used in a RFID system such as low frequency (125 KHz, 135 KHz), high frequency (13.56 MHz), ultrahigh frequency (400 MHz–960 MHz), and micro wave (2.45 GHz). According to the demands of transmission distance and speed, 433 MHz, 916 MHz, and 2.45 GHz are often used for container management. In China, 433 MHz can be used by radio amateur. At the same time, 860 MHz–960 MHz is the band belonging to GSM in China. So, radio signal whose frequency is 2.45 GHz is used in our system.

4.5. Firefighting Auxiliary Based on GPS Information. As introduced in Section 4.1, there are two ways to provide right firefighting knowledge according to the type of dangerous materials for fire crews. Firefighters can scan RFID tag on container by handhold terminal, and then the unique code of the container is transmitted to the object resolution server by transmit layer. The object resolution server identifies the container by unique code and extracts related information. The information includes the United Nations code (UN code) of the dangerous goods stored in the container and the monitoring service ID labeling the query service for the knowledge about firefighting. The information is submitted to the container yard monitoring server. The monitoring server queries the service rule database according to UN code and monitoring service ID. Then, firefighting knowledge is sent back to firefighter through handhold terminal by monitoring server.

If the tag on the container is destroyed, firefighter can report the location information of a slot to the object resolution server by the GPS function of the handhold terminal. The object resolution server deduces the slot number according to the location information first. The container stacked at that slot is identified further. The rest of the process is the same as the first method.

Table 2: Dangerous goods classified by hazardous properties.

Hazard properties	Code of division
Explosive	1.1, 1.4, 1.5, 1.6, 2.1, 5.1, 5.2
Flammable	Except for nonflammable goods
Toxic	2.3, 3, 6.1, 6.2, 9
Radioactive	7
Corrosive	8

The key issue for the second method is the way to deduce the slot number according to the location information. Location information about each slot is maintained in the object and service database. As a result, we can get a container's location range by slot number query and get slot number by location query. When the container is stored to a slot, the bond between the container unique code and slot number is built and recorded in the object and service database. So, we can get information about the dangerous goods in a container either by container number or by slot number.

Here, we only discuss the closed container. When we want to gain information about a certain container, we cannot put the handhold terminal into the container. The terminal can only be located near the container. As shown in Figure 5, there are three conditions for the relationship between the container and the handhold terminal:

(1) The height of the terminal is bigger than 2 tiers. According to the regulations in the recommendations on the transport of dangerous goods, height for containers of dangerous goods is no more than 2 tiers [30]. For condition (1.1), the container with slot number 01A03F02 is identified. For situation (1.2), because there is no container in tier 2, the slot number is 01A01F01.

(2) The horizontal coordinates of the terminal are out of the range of block. The container with slot number 01A04A01 is specified.

(3) For the third situation, the distances from the terminal to the containers with slot numbers 01A02C02, 01A03B02, and 01A02B01 are calculated, respectively. Suppose the distance to slot 01A02C02 is the shortest; the slot number 01A02C02 will be specified.

The deviation of open GPS supplied by USA is less than 10 meters. Researchers and manufacturers often improve the precision of GPS by difference algorithm. The application of carrier phase difference in GPS can bring about precision resolution in centimeters. The external dimensions of the most common container, 40GP, are $12192 \times 2438 \times 2591$ (mm). So, the resolution of GPS enhanced by difference algorithm can satisfy the location requirement in the container yard.

4.6. Environment Parameter Monitor and Control. Table 2 illustrates the hazardous goods classified by hazardous properties. According to the classification of dangerous goods introduced in Section 3.1 and Table 2, we can find out that explosion and flame are the main hazards of dangerous goods.

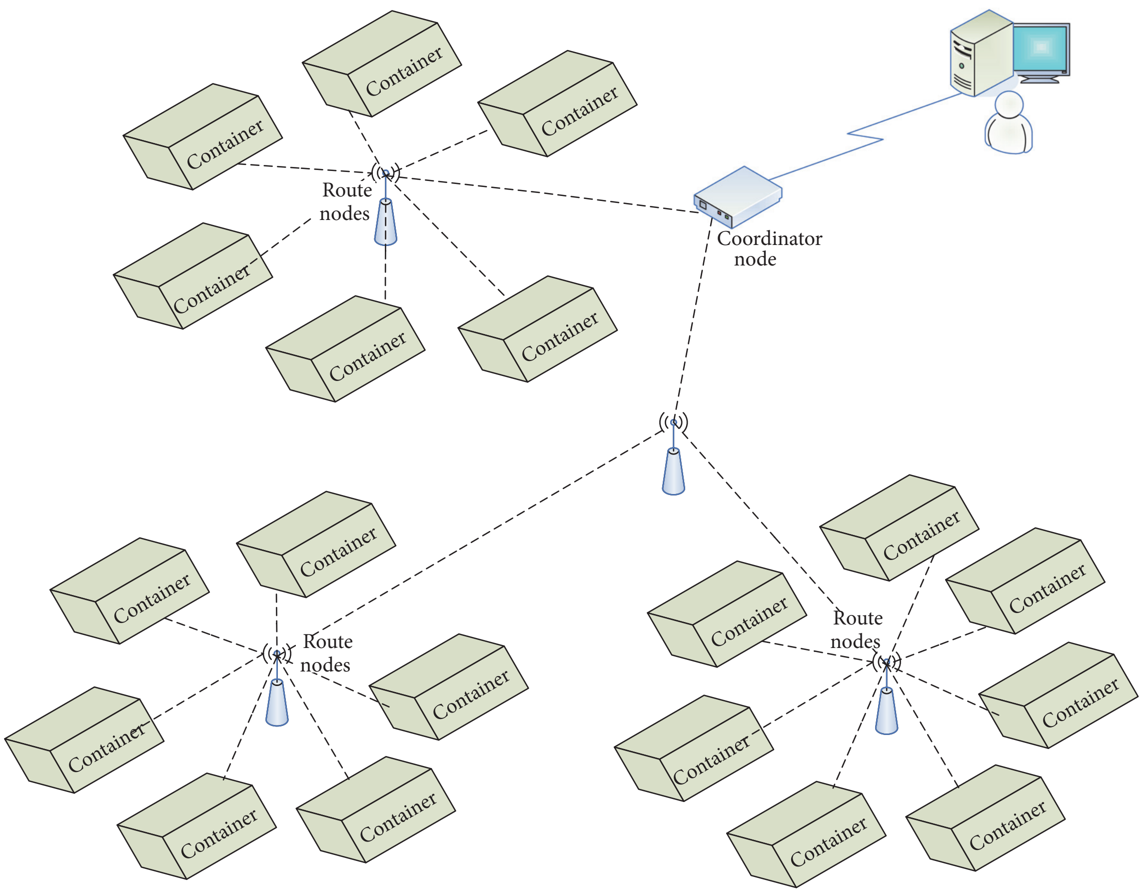

Figure 6: Schematic diagram of WSN for environment monitoring.

At the same time, there are many kinds of dangerous materials whose hazards are explosion and inflammation. Therefore, we emphasize the monitoring of explosion and inflammation in the container yard for dangerous materials. Generally, an explosion or flame needs three essential factors: combustibility, an oxidant, and temperature (ignition source). In extreme circumstances, the temperatures in containers may reach up to 50 Celsius or 70 Celsius. So the temperature is the key issue in these three elements.

As discussed before, temperature monitor and control are important for dangerous goods. This can be achieved with the support of wireless sensor networks. In order to get real-time temperature, temperature sensors should be mounted. There are two modes for the installation of temperature sensors: one temperature sensor is mounted in each container or several temperature sensors are installed at different places in the container yard. The first method needs the modification of container. It requires a large number of sensors. This method has an obvious advantage. Containers holding different kinds of dangerous goods can be monitored, respectively, according to the specific temperature requirements. This method can be enhanced to fulfill the control of humidity and CO_2 concentrations in dangerous goods containers. In order to reduce the number of sensors and simplify the installation process, compound sensor can be designed to collect information about temperature, humidity, and CO_2 concentrations.

Senor is the most important kind of monitoring node. For the first mode, monitoring node is mounted inside the container. Because the container itself has a strong shielding effect on the wireless signal, we fix antennas on the outer surface of the container door. A tree network is adopted in our system. As shown in Figure 6, the monitoring system consists of wireless sensor network and computer monitoring center. Except for sensors, there are two other kinds of monitoring nodes in the wireless sensor network. The coordinator node is responsible for the communication between the WSN and the computer monitoring center. It is the assignment for route nodes to transfer data and enlarge the coverage areas of the WSN. The monitoring nodes (sensors) collect related data, such as temperature and humidity, inside the container.

For the second way, temperature sensors are only deployed in container yard, so the outdoor temperature can be monitored with low cost. The monitoring system can also give some context-aware information. For example, when the outdoor temperature exceeds 30 degrees Celsius, it will notice the operators to spray the dangerous goods container every 2 hours.

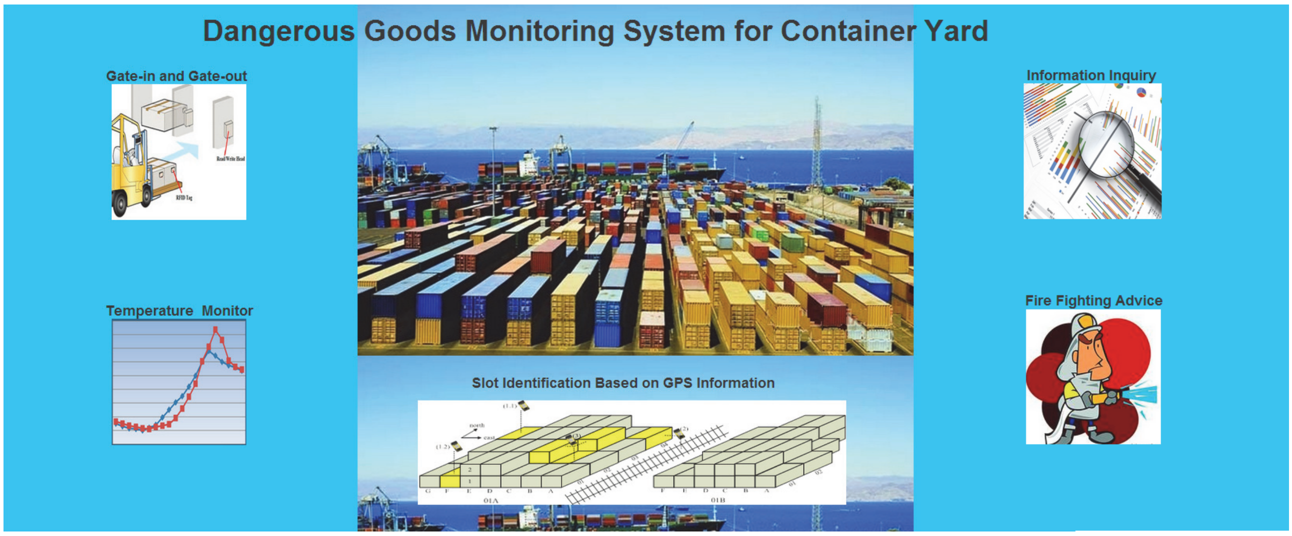

Figure 7: Main page of the prototype system.

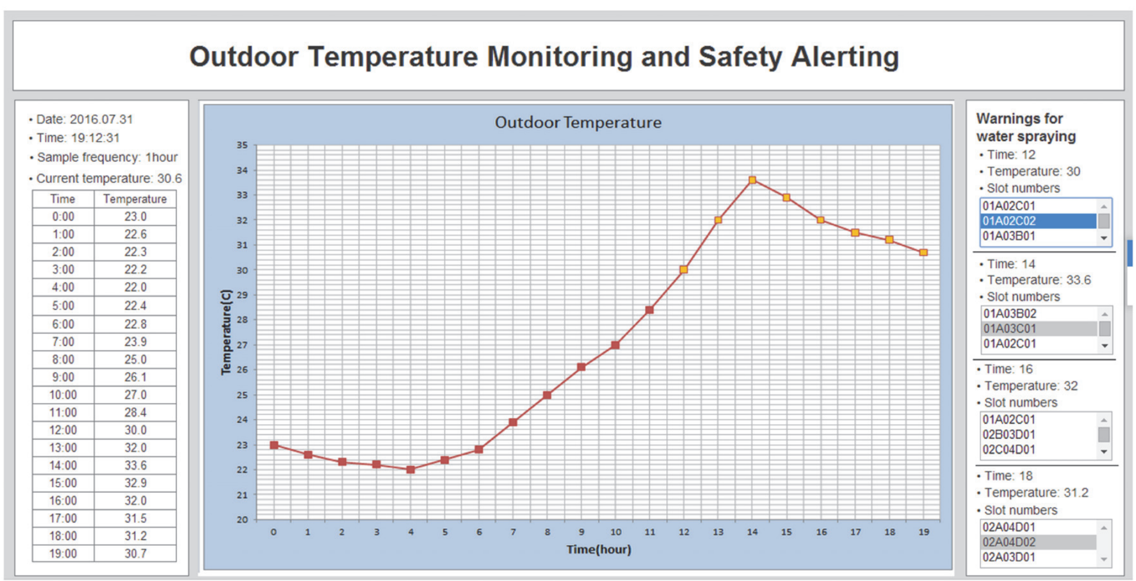

Figure 8: Function of environment parameter monitoring.

5. Prototype System

To verify the effect of our method, a prototype system is developed. Figure 7 shows the main page of the prototype system. The main functions including gate-in and gate-out management, temperature monitoring, firefighting auxiliary function, and information inquiry are implemented.

Temperature monitoring function is realized by the prototype system as the sample of environment parameters monitoring. As shown in Figure 8, outdoor temperature is collected each hour. At any time, the temperature can be browsed in table format or temperature curve. If the outdoor temperature is greater than or equal to 30 degrees Celsius, the corresponding dot in the temperature curve is painted in yellow. The right of Figure 8 lists the reminding information for spray. The reminding information is given following the rule introduced in Section 3 and is updated every 2 hours. The slot number of the containers that should be sprayed is listed as well.

Figure 9 is SHT11 intelligent sensor from Sensirion Company. It collects temperature and humidity in containers. It measures temperature with a resolution of 0.01 degrees and within ±2-degree accuracy and measures relative humidity with a resolution of 0.03% and within ±3.5% accuracy. The operating temperature range of SHT11 is from −40 to +125°C. The 2-wire serial interface and internal voltage regulation allow easy and fast system integration [31]. If electrochemical sensors are used to monitor concentration of gases such

Table 3: Field meaning of GPGGA message.

GGA	Global Positioning System Fix Data
123519	Fix taken at 12:35:19 UTC
4807.038,N	Latitude 48 deg. 07.038′ N
01131.000,E	Longitude 11 deg. 31.000′ E
1	Fix quality: 0 = invalid; 1 = GPS fix (SPS); 2 = DGPS fix; 3 = PPS fix; 4 = real-time kinematic; 5 = float RTK; 6 = estimated (dead reckoning); 7 = manual input mode; 8 = simulation mode
08	Number of satellites being tracked
0.9	Horizontal dilution of position
545.4,M	Altitude, meters, above mean sea level
46.9,M	Height of geoid (mean sea level) above WGS84 ellipsoid
(empty field)	Time in seconds since the last DGPS update
(empty field)	DGPS station ID number
*47	Checksum data, always beginning with*

Figure 9: SHT11, temperature and humidity sensor.

as nitric oxide and hydrogen sulfide, A/D modular should be designed to convert sensors' analogue signals to digital signals.

As introduced before, the right firefighting knowledge can be obtained by RFID tag on container or location information of container. Figure 10 shows the firefighting information got by location information through user terminal based on GPS function. The left part of Figure 10 is the location information, the slot number of the container identified according to the location information, and the firefighting principles for the dangerous goods in the container identified.

NMEA 0183 is a combined electrical and data specification for communication between GPS receivers. It has been defined and controlled by the National Marine Electronics Association. The baud rate supported by NMEA 0183 is 4800 bps, and all messages of NMEA-0183 are ASCII codes. Each message begins with a dollar sign ($) and ends with a carriage return and a linefeed (<CR><LF>).

Commonly used messages include GPGGA (Global Positioning System Fix Data), GPGSA (GPS DOP and active satellite), GPGSV (GPS Satellites in View), GPRMC (Recommended Minimum Specific DPS/Transit Data Speed), GPVTG (Track Made Good and Ground), and GPGLL (Geographic Position, Latitude/Longitude). GPGGA message can provide us with information such as time and position and fix related data. "$GPGGA,123519,4807.038,N,01131.000,E,1,08,0.9,545.4,M,46.9,M,,*47" is a GPGGA message. The meaning of each field is listed in Table 3.

The right part of Figure 10 lists the detailed information about the dangerous goods in the corresponding container. The information includes name, molecular formula, CAS number, UN number, type of hazard, and method of prevention and firefighting. It would help people to completely know the information about dangerous goods in the specific container.

6. Conclusion and Future Works

This paper proposes a framework for container yard of dangerous goods using IoT, monitoring environment parameters, and providing fire control service. It can reduce the risk of fire and explosion. When fire or explosion happens, firefighter can get right directions for firefighting through the fire control service. A prototype system is developed as well. Main functions of our method, such as gate-in and gate-out management, temperature monitoring, information inquiry, and firefighting auxiliary, are accomplished.

In the future, we will focus on the study of the storage assignment strategy for the dangerous goods in container yard. The assignment strategy must satisfy the regulations in recommendations on the transport of dangerous goods first of all [30]. We will accomplish the deployment of the system and investigate the quantitative benefits brought about by the system in our future work.

Competing Interests

The authors declare that there are no competing interests regarding the publication of this paper.

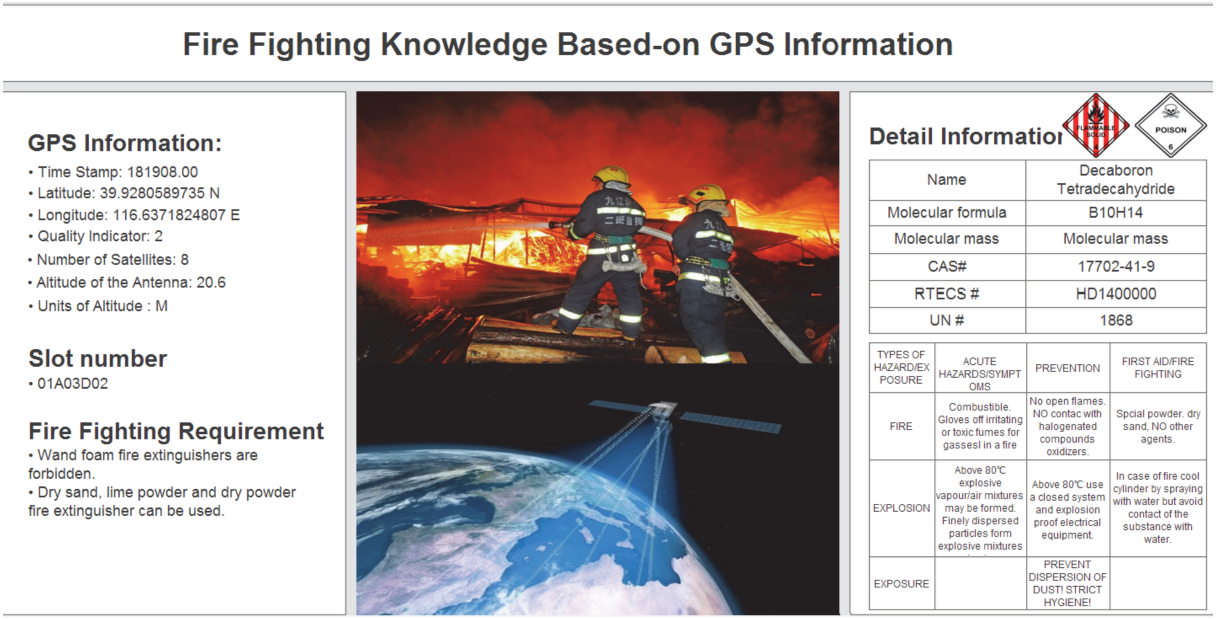

Figure 10: Firefighting knowledge obtained through location information.

Acknowledgments

This work was supported by Beijing Key Laboratory (no. BZ0211), Beijing Intelligent Logistics System Collaborative Innovation Center, and Breeding Project of BWU (Research of Logistics for Low Carbon Economy, no. GJB20162002).

References

[1] R. H. Weber, "Internet of Things—new security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, 2010.

[2] H. Ning and Z. Wang, "Future internet of things architecture: like mankind neural system or social organization framework?" *IEEE Communications Letters*, vol. 15, no. 4, pp. 461–463, 2011.

[3] "ITU internet report 2005: the internet of things," Tech. Rep., International Telecommunication Union, 2005.

[4] F. Pramudianto, I. R. Indra, and M. Jarke, "Model driven development for internet of things application prototyping," in *Proceedings of the International Conference on Software Engineering and Knowledge Engineering*, Boston, Mass, USA, June 2013.

[5] Wikipedia, "2015 Tianjin explosions," 2015, https://en.wikipedia.org/wiki/2015_Tianjin_explosions.

[6] R. Fergus, "Tianjin explosions: warehouse 'handled toxic chemicals without licence'—reports," The Guardian, https://www.theguardian.com/world/2015/aug/18/tianjin-blasts-warehouse-handled-toxic-chemicals-without-licence-reports.

[7] R. Iyengar, "Searching questions asked in the aftermath of the Tianjin blasts," Time, August 2015.

[8] "Report on the investigation of the explosion accident in Tianjin port," Phoenix Information, 2016.

[9] J. P. Conti, "The internet of things," *IET Communications Engineer*, vol. 4, no. 6, pp. 20–25, 2006.

[10] ITU, "The Internet of Things," ITU International Reports, 2005.

[11] INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems Groups in Co-Operation with the RFID Working Group of the EPoSS, "Internet of Things in 2020", 2008.

[12] Coordination and Support Action for Global RFID-Related Activities and Standardization (CASAGRS), "RFID and the inclusive model for the internet of things," CASAGRAS Final Report, 2009.

[13] Cluster of European Research Projects on the Internet of Things (CERPIoT), *CERP-IoT Research Roadmap*, 2009.

[14] Cluster of European Research Projects on the Internet of Things (CERPIoT), *Vision and Challenges for Realising the Internet of things*, 2010.

[15] IBM Institute for Business Value, "A Smart Planet," 2009, http://www.ibm.com/smarterplanet/us/en.

[16] F. Thiesse, C. Floerkemeier, M. Harrison, F. Michahelles, and C. Roduner, "Technology, standards, and real-world deployments of the EPC network," *IEEE Internet Computing*, vol. 13, no. 2, pp. 36–43, 2009.

[17] G. Broll, M. Paolucci, M. Wagner, E. Rukzio, A. Schmidt, and H. Hussmann, "Perci: pervasive service interaction with the internet of things," *IEEE Internet Computing*, vol. 13, no. 6, pp. 74–81, 2009.

[18] J. I. Vazquez, J. Ruiz-De-Garibay, X. Eguiluz, I. Doamo, S. Rentería, and A. Ayerbe, "Communication architectures and experiences for web-connected physical smart objects," in *Proceedings of the 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops '10)*, pp. 684–689, Mannheim, Germany, April 2010.

[19] L. Yan, Y. Zhang, L. T. Yang, and H. S. Ning, "The internet of things: from RFID to the next-generation pervasive networked systems," *Journal of Vertebrate Paleontology*, vol. 15, no. 2, pp. 431–442, 2010.

[20] É. Renault, A. Ahmad, and M. Abid, "Toward a security model for the future network of information," in *Proceedings of the 4th*

International Conference on Ubiquitous Information Technologies and Applications (ICUT '09), pp. 1–6, IEEE, Fukuoka, Japan, December 2009.

[21] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.

[22] S. Bin, L. Yuan, and W. Xiaoyi, "Research on data mining models for the internet of things," in *Proceedings of the 2nd International Conference on Image Analysis and Signal Processing (IASP'10)*, pp. 127–132, April 2010.

[23] H. Ning, N. Ning, S. Qu, Y. Zhang, and H. Yang, "Layered structure and management in internet of things," in *Proceedings of the International Conference on Future Generation Communication and Networking (FGCN '07)*, vol. 2, pp. 386–389, Jeju Island, Korea, December 2007.

[24] Future Internet Assembly, "Towards the future Internet: emerging trends from European research," http://www.future-internet.eu/home/future-internet-assembly.html.

[25] EPCglobal, "The EPCglobal Architecture Framework," final version 1.3, 2009.

[26] S. Sarma, D. L. Brock, and K. Ashton, "The networked physical world: proposals for engineering the next generation of computing, commerce & automatic-identification," White Paper MIT-AUTOID-WH-001, MIT Auto-ID Center, 2010.

[27] N. Koshizuka and K. Sakamura, "Ubiquitous ID: standards for ubiquitous computing and the internet of things," *IEEE Pervasive Computing*, vol. 9, no. 4, pp. 98–101, 2010.

[28] E. Welbourne, L. Battle, G. Cole et al., "Building the internet of things using RFID: the RFID ecosystem experience," *IEEE Internet Computing*, vol. 13, no. 3, pp. 48–55, 2009.

[29] R. Want, "An introduction to RFID technology," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 25–33, 2006.

[30] ONU, "Recommendations on the transport of dangerous goods: model regulations," 2005.

[31] SHT71 datasheets and info, https://www.sensirion.com/en/products/humidity-sensors/digital-humidity-sensors-for-accurate-measurements/.