International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org || PP. 55-61

Extending Internet of Things (IoT): 5G scenario with Security and Application

Dr.S.VENNILA[1]
[1]*(Assistant Professor & Head in Computer Application St.Ann's College of Arts and Science Tindivanam)*

Abstract: *The Internet of Things (IoT) is a powerful paradigm that has made progress in the almost every field of human life. This paper gives an overview of IoT, its enabling technologies, applications and security issues in the wireless technologies. IoT is enabled by a number of different technologies such as Radio Frequency Identifiers (RFID), and Wireless Sensor Networks (WSN) with 5G. There are huge number of applications of IoT in almost every aspect of life i.e. healthcare, logistics and supply chain management, smart environment and social application etc. only a few of these applications are discussed in this paper. Security is an important concern of wireless networks and so it is one of the main issues in IoT. This paper gives an Extending IoT-5G scenario with security and application concerns in an IoT system and methods to prevent those issues.*
Keywords: *Internet of Things (IOT), RFID, WSN, SOA, 5G, CDMA*

I. Introduction

To date, a huge number of devices such as computers and mobile handsets used directly by humans communicate through worldwide Internet connections. The communication of this form is called Human-to-Human. In a not so far future, every object can be connected via Internet. The future is not going to be people talking to people, but it is going to be machines talking to other machines on account of the user. We are entering the era of IoT in where new forms of interaction between human and things, and also between things themselves is going to be realized, therefore adding a new aspect to the world of information technology and Communication.

Internet of Things (IoT) is an innovative paradigm that is making ground in the setup of modern wireless telecommunications rapidly. The basic impression of this concept is the extension of Internet into real world by taking up everyday objects. Physical agents are no longer separated from the virtual world but are controlled remotely acting as physical contact points to Internet services.

The IoT is not a new concept in the industry. In his 1999 article for RFID Journal [3], Kevin Ashton defined Internet of Things as "If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count.

Everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory".

The definition of Kevin Ashton was in the background of supply chain management. Nonetheless, the wide range of applications has made the definition more inclusive. Although, the description of 'Things' has changed with the evolution of technologies, the focal point of computer sensing information without human aid remains the unchanged. A profound evolution of current Internet into a network of interconnected objects which not only collect information through sensing and interacting with the physical world, but also employ current internet standards to deliver services for information transfer, communications, applications, and analytics. Open wireless technologies such as Bluetooth, RFID, and Wi-Fi; have led IoT from its infancy to the verge of fully. renovating the current Internet into a fully incorporated future Internet.

Undoubtedly, the main strength of IoT is its high impact on numerous aspects of routine lifestyle and actions of the potential users. The success of IoT from the point of view of a private user will be evident in both domestic and working fields. In this situation, e-Health, assisted living, enhanced learning are few of many possibilities where the new paradigm will play a leading role. From the business user's perspective, the most important applications will be in automation and industrial manufacturing, intelligent transportation, logistics, and process management.

The purpose of this paper is to define the concept of Internet of Things, its enabling technologies, and the use of these technologies in context of its basic applications and to create low-cost and low-power systems for efficient monitoring of critical data in remote areas and providing efficient services to the users. Also this paper discusses the main threats and attacks to the security of IoT system, and gives a brief overview of the cryptographic techniques used in sensor networks to provide information security in an IoT environment.

The rest of paper is organized as follows: Section II provides a comprehensive survey of the enabling technologies actuating the concept of IoT in real world. Section III Discusses the major application areas of IoT and some of their implementations. Security attacks on the wireless technologies involved in IoT and their countermeasures are discussed in section IV. Lastly we discuss the conclusion of our discussion and future work in the field of IoT.

II. Key Technologies Involved In Internet Of Things

Realization of the IoT model into the real world is achievable through the assimilation of a number of enabling technologies.

A. Wireless Technologies

Now-a-days the wireless technologies are playing a vital role in our lives. Radio-Frequency Identification systems are the vital components of internet of things, which are composed of several RFID tags and more than one reader. Tags are distinguished by a unique identifier and are subjected to objects. By generating suitable signal, readers activate the Tag transmission, which illustrate a query for the potential occurrence of tags in the adjacent area and for the response of their IDs. From a manufacturing point of view, the RFID tag is a small microchip attached to an antenna in a suite which usually is similar to an adhesive sticker [6]. There are two types of RFID Tags: passive RFID Tags and active RFID Tags. Passive RFID Tags do not have onboard power supplies whereas active RFID Tags are getting power supply from batteries.

In the field of IoT sensor networks have played a fundamental role. These days sensor networks with the collaboration of RFID systems are used to trail the status of things in environment, i.e., their movements, location, temperature etc. The employment of sensor networks has been projected in numerous applications, such as intelligent transportation systems, e-health care monitoring, environmental/earth monitoring, military, and industrial plant monitoring. Sensor networks composed of a certain number of sensing nodes which communicate in a wireless multi-hop fashion. Generally nodes report the outcomes of their sensing to a small number of special nodes called sinks [5].

B. IoT Architecture Technology Middleware

The IoT middleware is a software layer composed of a set of sub-layers placed between the technical and the application levels. The fundamental property of hiding the various technological details in middleware allows the programmer to free from problems that are not directly relevant to his focus, which is the development of the particular application enabled by the IoT infrastructures.

The middleware architectures for the IoT follow the Service Oriented Architecture (SOA) approach. The realization of the SOA principles allows for decomposing composite systems into applications consisting of simpler and well-defined components. A SOA approach also permits for reusing of both hardware and software, because it does not require a fixed technology for the service implementation.

The middleware relies on the layers explained as follows:

1) Application Layer

Applications are present on top of the structural design, providing all the system’s functions to the user. Indeed, application layer is not deliberated to be part of the middleware but use all the functions provided by the middleware layer.

2) Service Composition Layer

Service composition layer is usually the upper layer of the SOA middleware. The main function of this layer is provided, the simple configuration of single services presented by network objects represented in order to build certain applications. In this layer creation and management of complex services, can be seen with respect to the flow of business processes with workflow languages like Business Process Execution Language (BPEL) and Jolie [10].

3) Service Management Layer

Service management layer offers the key features that should be available to every object and allows the management of each object in IoT framework. A fundamental set of services includes: status monitoring, service settings and object dynamic discovery. In order to meet the needs of the application of this layer it provides remote use of new services during process time. Service management layer also includes an enhanced set of functionalities associated to the Quality of service management, lock management, etc. At this layer a storing mechanism is present to know the records of services allied to each object in network [5].

4) Object Abstraction Layer

The Internet of things depends on broad and heterogeneous objects, each to achieve the provision of certain functions on their own dialect. So an abstraction layer is able to access the diverse devices with a mutual language and the process of harmonization required. Therefore, unless a device provides detectable Web services over an IP network, it is necessary to introduce a cladding layer consisting of two sub-layers: the communication sub-layer and the interface layer. The interface layer provides a web interface exposes methods through a standard Web services interface is available and is responsible for managing all incoming mail / outgoing communication with the outside world involved responsible. The communication sub-layer is responsible for the reasoning behind the web service techniques and translation of these methods in a specific set of commands to the device to interact with objects in the real world [10].

5) Trust, Confidentiality and Security Management

The incorporation of electronic communication objects in our lives a threat to our future. Therefore middleware functions should ally for the managing trust, confidentiality and security of all data exchanged. The corresponding functions can be either on a particular layer of the foregoing, or (often happens) distributed throughout the stack, from object abstraction to the service composition in a fashion that does not disturb system performance or introduce excessive overheads.

III. Applications of Iot

The development of a number of applications of IoT has been made possible because of the potentials offered by this field. Only a small number of these applications have been made available to the society. There are a number of domains and environments in which the applications of IoT can improve our lives. Based on the review of literature for this paper, the applications of IoT can be classified into following application areas: healthcare, logistics and supply chain, and smart environment, personal and social applications.

A. Healthcare

Healthcare applications are one of the major fields of IoT. The new breed of low-cost, low-power communication devices have made it possible for the everyday objects to be part of the ncccetworks making Internet of Things. Similar advancements are made in electronic healthcare solutions, especially in wearable sensors and HealthCare Record (HCR) databases and formats [11]. IoT technologies provide many benefits in healthcare domain that can be grouped as: staff tracking and patients tracking, identification of healthcare personnel and authentication, sensing and collecting data [5].

In [12], RFID technology is used to build smart hospitals. It also demonstrates RFID Locator technology which is a web-based application allowing the tracking of assets within a predefined area. RFID Locator is scalable and robust distributed application.

A wireless localization system is presented in 2008 that tracks location of patients and monitor their physical status. The localization network is implemented using Fleck Nano wireless sensor platform for mobile inertial movement sensing [13]. The localization network consists of static nodes, mobile nodes and base nodes. The static node is

B.Logistics and supply chain management

The role of RFID and Sensors in the field of supply chains has been established for a long time. Assembly lines of manufacturing facilities have been using sensors and RFID generally to track products in supply chain controlled by an enterprise. The IoT can enhance logistics and supply chain competence by providing detailed and up-to-date information about raw material purchase, production, transportation, storage, distribution, etc.

Perishable goods are important part of our daily nutrition. The conservation status of these products needs to be monitored in order to maintain an efficient food supply chain. The simulation model defined in [18] describes the study of the quality of perishable things at a dealer under diverse issuing policies at the distributor. The expiry dates and product quality is automatically collected using RFID sensors to improve quality of objects in stores.

The system proposed in [19] uses integration of WSN and Barcode reader for real-time tracking of products information and code reading. It also gives a reference mathematical model for studying upper and lower limits of inventory for achieving faster, reliable and efficient management of supermarkets.

Logistic Geographical Information Detecting Unified Information System Based on Internet of Things in [20] integrates mobile telecom technology, RFID, GPS and perception technology for real time perception.

ALMA presented in [21] combines 3G and High Performance Computing (HPC) infrastructure to provide high quality mobile logistic services. The HPC infrastructure consists of: a *broker* for selecting an appropriate HPC infrastructure among several available distributed or parallel architectures, and the computing environment.

In [22], authors present an RFID based system called RF-compass for robot navigation and object management. When an RFID tagged object is provided, the RF-Compass precisely navigates an RFID equipped robot towards the object. The center position and orientation of objects can be pointed out by RF-Compass with an accuracy of 80-90%. The key innovation of this system is the iterative algorithm, using RFID signals for space partition based on continuous movement of robot.

C. Smart Environments

Internet of Things hosts the prophecy of ubiquitous computing and ambient intelligence increasing them by needing a complete communication and a comprehensive computing anytime, anywhere, with anything and anyone supremely by means of any network and any service [23]. In general, the vision of "smart environment" comprises of utilizing the current Information and Communication Technologies (ICT) in performing public affairs. The main aim of smart environment is to make improved use of resources and services accessible to citizens and providing good quality of life in industrial plant, homes and offices etc.

A surveillance system is introduced in [24] based on internet of things for oil depot with the intention of providing safety management. The proposed system is composed of three layers: the sensing layer consists of RFID tags and explosion-proof personal digital assistants (PDAs) used to distinguish and intermingle with main services in oil depot. The communication layer is used to link worksite and internet in order to transfer data via 3G between user and internet. Through this the workers easily accessed the safety management information.

In [25], is presented a smart environment in which smart heat and electricity management system is used to monitor real-time electricity consumption of buildings and individual appliances. In this system smart meters are used for enabling automatic energy management and data recorders. Based on IoT technologies for information authentication and recognition, if the energy consumption of objects was above the limits then users will be informed of this abnormal situation.

D.* Social Internet of Things (SIoT*)

Current communication requirements of the society involve not only humans but also things, thus creating an IoT environment where entities have virtual equivalents on the Internet. These virtual entities not only use services, but also work towards common objectives and must be connected with all other services. To provide these entities the possibility of efficient communication, a new standard is needed. It is evident from scientific research that a great number of individuals connected via social network deliver more precise results to complex problems than an individual working on the same problem. The merging of IoT and social networking has directed to a novel concept called Social Internet of Things (SIoT) [28], where objects act like humans to generate their own relationships based on the rules set by their masters. While practical implementations of IoT are already available for use, the SIoT is still afield of pure exploration and simulations.

MULTImedia-supported Social Web of Things (MUL-SWoT) provides easy incorporation of smart objects and 3rd party service providers for providing innovative IoT services recommendations and handling user data [29]. MUL-SWoT consists of five key elements i.e. Home Objects, Social Network, Smart Home Gateway, 3rd party service provider and MUL-SWoT platform, performing different roles. An Intrusion Detection System (IDS) is built on top of MUL-SWoT for practical demonstration. The purpose of IDS is to observe homes and detect any possible intrusions, and attacks on the property, and notifying user about the status of the property by posting messages on Facebook wall of the user.

Like Art[30] is another case in which social media and IoT are incorporated. Visitors are able to indicate their favorite artwork by just a wave of hand read through sensors attached to the object.

An Object Oriented method for SIoT is presented in [31], and its implementation on Android based Smart office is also defined. The relationships about nodes, class, owner and entity object are defined, along with six basic attributes and three methods to organize entity objects. The smart office application uses the sensor data and sends messages to the user through a cloud server on social media, which in this case is WeChat.

IV. Wireless Technology Security Issues

In the scenario of the existing Internet, many protocols and tools are available to meet many of the security problems, but applicability of existing tools in the field of IoT are limited due to restrictions on the IoT hardware nodes and wireless sensor networks. Another factor which limits the realization of present security tools is that the IoT devices typically have to perform in extreme, erratic, and hostile surrounding environments, which can be susceptible to damage and despicable intentions. Thus, the realization of the existing security tools continues to be a demanding task.

Machine to machine communication: has a significant role to play in emerging internet of things paradigm in years and decades to come. The emerging IoT-5G scenario extends sensor based IoT capabilities to robots, actuators and drones for distributed coordination and low-latency reliable execution of tasks at hand. In the invited work titled "Enabling the IoT machine age with 5G: Machine-type multicast services for innovative real-time applications" by Condoluciett al., core attention is focused on the end-to-end reliability, latency, and energy consumption comprising both up and downlinks for 5G-IoT communication. The authors propose the definition, design, and analysis of machine-type multicast service (MTMS). They recommend different procedures that need to be redesigned for MTMS and derive the most appropriate design drivers by analyzing different performance indicators, such as scalability, reliability, latency, and energy consumption. Overall, a very interesting read complemented by open problems and future research directions to pursue.

Security is one of the biggest challenges faced by Internet of Things. With devices becoming ubiquitous and pervasive in day to day lives necessitate reliable and secure algorithms. The third article, "Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations" by Xu et al., develops a secure framework for eavesdroppers with Uncertain Locations in IoT. With the assumption that the locations of eavesdroppers change independently from hop to hop, authors derive an expression for the secrecy outage probability of the two-hop transmission, which is shown to be the upper bound of the outage probability when the locations of eavesdroppers remain unchanged. Following this expression, the end users formulate a secrecy rate maximization problem with the secrecy-outage probability constraint. The optimal rate design for codebooks and power allocation between the source and relay are derived. By studying the performance of the optimal scheme in some special cases, we obtain several insights concerning the setting of system parameters.

Enabling massive IoT in 5G and beyond systems: PHY radio frame design considerations" by Ayesha Ijaz et al., the authors propose a flexible frame structure and design for massive Internet of Things (IoT) devices working in 5G wireless network. The authors also discussed the interdependence of different frame design parameters, service requirements and characteristics of radio environment. Based on these interdependency, they provide guidelines for radio numerology design and elaborated on the frame design for IoT communications in 5G networks to support massive connection density of low-rate, low-power devices. The article concludes with some key research findings and challenges massive IoT in 5G wireless network.

It is estimated that in year 2020, 20 to 40 billion devices will be connected to the Internet as part of the Internet of Things. A critical bottleneck for realizing the efficient IoT is the pressure it puts on the existing communication infrastructures, requiring transfer of enormous data volumes. In the article "CONDENSE: A reconfigurable knowledge acquisition architecture for future 5G IoT", by Dejan Vukobratovic et al., the authors propose a architecture named 'Condense' which integrates the acquisition of IoT-generated data within the 3GPP MTC (machine type communications) systems. The proposed Condense architecture introduces a service within 3GPP MTC systems – computing linear and non-linear functions over the data generated by MTC devices This service brings about the possibility that the underlying communication infrastructure communicates only the desired function of the MTC- generated data (as required by the given application at hand), and not the raw data in its entirety. This transformational approach has the potential to dramatically reduce the pressure on the 3GPP MTC communication infrastructure. The article concludes by discussing challenges, provides insights, and identifies future research directions for implementing function computation and function decomposition within practical 3GPP MTC systems.

"Frequency-domain oversampling for cognitive CDMA systems: Enabling robust and massive multiple access for Internet of Things" by Su Hu et al., the authors utilize the concept of cognitive radio with dynamic non-continuous spectrum bands and code division multiple access to tackle the challenge of massive spectrum resource management in IoT. In order to suppress multiple access interference resulting from the non-orthogonality of partial available spectrum bins, carrier frequency offset, and spectrum sensing mismatch, the authors propose an enhanced receiver design that combines the frequen6-domain oversampling scheme (FDO) and linear minimum mean square error (MMSE) method. The simulation results show that the cognitive-CDMA with FDO-MMSE receiver outperforms that with conventional per-user MMSE receiver in the presence of multipath fading channels, carrier frequency offset, and spectrum sensing mismatch. "A survey of client-controlled HetNets for 5G" by Michael Wang et al., a comprehensive review is provided on spectrum of client-controlled HetNets for 5G networks: from the fully devolved distributed local control approach to the hybrid control approach where clients may make the decisions given some global information provided by the network. After giving a thorough review, the authors also provide future research directions and recommendations for evolution of 5G heterogeneous networks as an enabler for next generation internet of things.

Cryptography in Sensor Networks

Since sensor nodes have limited storage and computational resources, the traditional methods of Internet security are too expensive for sensor networks. As all the security services are provided by cryptography, therefore selection of proper cryptographic method is extremely important in sensor networks [37].

There are two types of cryptography: Symmetric key cryptography and Asymmetric key cryptography. A single key is used for both encryption and decryption in symmetric key cryptography, while asymmetric key cryptography uses separate keys for encryption and decryption [39].

Use of encryption algorithms, key distribution policies, intrusion detection mechanism and security routing policies, can help minimize the security threats to the sensor networks [32]. These methods are explained below:

a) **Key management:** it is an important and complex issue in symmetric key cryptography. Several schemes are proposed for solving this issue, the most common being the key pre-distribution schemes, which distributes keys onto sensor nodes before deployment. The sensor nodes can use these keys for secure communication setup after deployment.

Key pre-distribution schemes are further divided into two types based on the possibility of sharing keys between two sensor nodes: deterministic and probabilistic. The main idea of probabilistic scheme is to pre-load each sensor randomly with a subset of keys from the key pool before deployment. On contrary, deterministic scheme guarantees that the two intermediate nodes share one or more pre-distribution keys.

b) **Secure routing strategies:** Data routing and forwarding is a vital service for establishing communication in wireless sensor networks. There are several security issues in routing data. In order to improve security, many routing protocols are being designed especially for sensor networks. According to network structure, these protocols are classified as [39]: flat-based routing, hierarchical-based routing, and location-based routing. Equal functionality is assigned to all nodes in flat-based routing. In hierarchical-based routing, different roles are played by nodes in the network. In location-based routing, the positions of sensor nodes are used to route data across network.

A number of security routing strategies are proposed, including multi-path routing policy which is used to counter forwarding attacks. Also by limiting the routing of nodes to a specific range data, flooding attacks can be minimized.

c) **Intrusion detection mechanism:** Sensor networks are vulnerable to many forms of intrusions. When the security flaw is detected in sensor networks, the intrusion detection mechanism provide additional security layer in IoT and suitable security remedies are provided [43], [44]. These mechanisms monitor network for suspicious activities against normal behavior.

V. Conclusion

Internet of things is an emerging field which has improved the quality of human life with its vast automated applications. The functionalities provided by IoT can save time and computational power of users to help improve results in the diverse application areas. This paper presented The Extending IoT-5G scenario with security and application . Further, some of the security issues regarding the wireless technologies involved in deployment of IoT are presented along with their possible counter measures. The future of internet is IoT, but there is still a need for further research in this field because of the ever increasing demands of users.

References

[1]. T. Lu and W. Neng, "Future internet: The Internet of Things," in *Advanced Computer Theory and Engineering (ICACTE), 2010 3rd International Conference on*, 2010, pp. V5-376-V5-380.

[2]. M. H. Asghar, N. Mohammadzadeh, and A. Negi, "Principle application and vision in Internet of Things (IoT)," in *Computing, Communication & Automation (ICCCA), 2015 International Conference on*, 2015, pp. 427-431.

[3]. K. Ashton, "That 'Internet of Things' Thing," *RFID Journal*, 2009.

[4]. J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems,* vol. 29, pp. 1645-1660, 9// 2013.

[5]. L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Computer Networks,* vol. 54, pp. 2787-2805, 10/28/ 2010..

[6]. A. Juels, "RFID security and privacy: a research survey," *Selected Areas in Communications, IEEE Journal on,* vol. 24, pp. 381-394, 2006.

[7]. S. de Deugd, R. Carroll, K. E. Kelly, B. Millett, and J. Ricker, "SODA: Service Oriented Device Architecture," *Pervasive Computing, IEEE,* vol. 5, pp. 94-96, 2006.

[8]. J. Pasley, "How BPEL and SOA are changing Web services development," *Internet Computing, IEEE,* vol. 9, pp. 60-67, 2005.

[9]. P. Spiess, S. Karnouskos, D. Guinard, D. Savio, O. Baecker, L. Souza, *et al.*, "SOA-Based Integration of the Internet of Things in Enterprise Services," in *Web Services, 2009. ICWS 2009. IEEE International Conference on*, 2009, pp. 968-975.

[10]. C. Buckl, S. Sommer, A. Scholz, A. Knoll, A. Kemper, J. Heuer, *et al.*, "Services to the Field: An Approach for Resource Constrained Sensor/Actor Networks," in *Advanced Information Networking and Applications Workshops, 2009. WAINA '09. International Conference on*, 2009, pp. 476-481.

[11]. N. Bui and M. Zorzi, "Health care applications: a solution based on the internet of things," presented at the Proceedings of the 4th

International Symposium on Applied Sciences in Biomedical and Communication Technologies, Barcelona, Spain, 2011.

[12]. P. Fuhrer and D. Guinard, "Building a Smart Hospital using RFID Technologies," *ECEH*, vol. 91, pp. 131-142, 2006.

[13]. M. D'Souza, T. Wark, and M. Ros, "Wireless localisation network for patient tracking," in *Intelligent Sensors, Sensor Networks and Information Processing, 2008. ISSNIP 2008. International Conference on*, 2008, pp. 79-84.

[14]. A. K. Chandra-Sekaran, P. Dheenathayalan, P. Weisser, C. Kunze, and W. Stork, "Empirical Analysis and Ranging Using Environment and Mobility Adaptive RSSI Filter for Patient Localization during Disaster Management," in *Networking and Services, 2009. ICNS '09. Fifth International Conference on*, 2009, pp. 276-281.

[15]. A. A. N. Shirehjini, A. Yassine, and S. Shirmohammadi, "Equipment Location in Hospitals Using RFID-Based Positioning System," *Information Technology in Biomedicine, IEEE Transactions on*, vol. 16, pp. 1058-1069, 2012.

[16]. S. Tennina, M. Di Renzo, E. Kartsakli, F. Graziosi, A. Lalos, A. Antonopoulos, *et al.*, "WSN4QoL: a WSN-oriented healthcare system architecture," *International Journal of Distributed Sensor Networks*, vol. 2014, 2014.

[17]. C. Occhiuzzi, C. Vallese, S. Amendola, S. Manzari, and G. Marrocco, "NIGHT-Care: a passive RFID system for remote monitoring and control of overnight living environment," *Procedia Computer Science*, vol. 32, pp. 190-197, 2014.

[18]. A. Dada, Fr, #233, #233, and r. Thiesse, "Sensor applications in the supply chain: the example of quality-based issuing of perishables," presented at the Proceedings of the 1st international conference on The internet of things, Zurich, Switzerland, 2008.

[19]. L. Renwang, L. Hao, and B. Zhigang, "Based on the Internet of things the supermarket chain management information system development and safety stock research," in *Education Technology and Computer (ICETC), 2010 2nd International Conference on*, 2010, pp. V2-368-V2-371.

[20]. L. Xingzhi, "Logistic geographical information detecting unified information system based on Internet of Things," in *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*, 2011, pp. 303-307.

[21]. D. El-Baz, J. Bourgeois, T. Saadi, and A. Bassi, "ALMA, A Logistic Mobile Application Based on Internet of Things," in *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing*, 2013, pp. 355-358.

[22]. J. Wang, F. Adib, R. Knepper, D. Katabi, and D. Rus, "RF-compass: robot object manipulation using RFIDs," presented at the Proceedings of the 19th annual international conference on Mobile computing & networking, Miami, Florida, USA, 2013.

[23]. A. W. Burange and H. D. Misalkar, "Review of Internet of Things in development of smart cities with data management & privacy," in *Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in*, 2015, pp. 189-195.

[24]. D. Zhigao, M. Yaming, and L. Ming, "Design and Implementation of Safety Management System for Oil Depot Based on Internet of Things," in *Green Computing and Communications (GreenCom), 2012 IEEE International Conference on*, 2012, pp. 249-252.

[25]. White, and J. Cooper, "Sustainable smart city IoT applications: Heat and electricity management & Eco-conscious cruise control for public transportation," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a*, 2013, pp. 1-5.

[26]. X. Yun, C. Xiaojiang, W. Lin, L. Wei, L. Baoying, and F. Dingyi, "An Immune Theory Based Health Monitoring and Risk Evaluation of Earthen Sites with Internet of Things," in *Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing*, 2013, pp. 378-382.

[27]. Q. Chi, H. Yan, C. Zhang, Z. Pang, and L. Da Xu, "A reconfigurable smart sensor interface for industrial WSN in IoT environment," *Industrial Informatics, IEEE Transactions on,* vol. 10, pp. 1417-1425, 2014.

[28]. R. Girau, M. Nitti, and L. Atzori, "Implementation of an Experimental Platform for the Social Internet of Things," in *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on*, 2013, pp. 500-505.

[29]. C. Tein-Yaw, I. Mashal, O. Alsaryrah, C. Chih-Hsiang, H. Tsung-Hsuan, L. Pei-Shan, *et al.*, "MUL-SWoT: A Social Web of Things Platform for Internet of Things Application Development," in *Internet of Things (iThings), 2014 IEEE International Conference on, and Green Computing and Communications (GreenCom), IEEE and Cyber, Physical and Social Computing(CPSCom), IEEE*, 2014, pp. 296-299.

[30]. A. Sanchez Pineda, Maranon-Abreu, R. (2014). *Like Art: Integrating Internet of Things and Social Networks*. Available: http://like-art.com/