The Internet of Things: Challenges & Security Issues

Gurpreet Singh Matharu
Department of Information Technology
Amity University Uttar Pradesh
Noida, India
mtech.gurpreet@gmail.com

Priyanka Upadhyay
Department of Information Technology
Amity University Uttar Pradesh
Noida, India
priyanka.upadhyay0991@gmail.com

Lalita Chaudhary
Department of Information Technology
Amity University Uttar Pradesh
Noida, India
lalita.chaudhary19@gmail.com

***Abstract*—Propelled by large-scale advances in wireless technologies, sensing technologies and communication technologies, the transformation of the Internet into an integrated network of things termed as Internet of Things is rapidly unfolding. The Internet of Things enabled by Wireless Sensor Networks (WSN) and RFID sensors finds a plethora of applications in almost all the fields such as health, education, transportation and agriculture. This paper briefs the idea of Internet of Things (IoT) and the challenges to its future growth. Also, this paper describes the general layered architecture of IoT along with its constituent elements. Further, the paper provides for a secure construction of the IoT architecture, by tackling security issues at each layer of the architecture. The paper concludes by mentioning the potential applications of the IoT technologies in fields ranging from intelligent transportation to smart home to e-health care and green agriculture.**

Keywords—Internet of Things (IoT); RFID; Security; Architecture.

I. INTRODUCTION

Internet of Things (IoT) is the next era in the IT world which would take the technology to new heights. IoT takes the internet from its infancy and transforms it into a fully integrated form of Internet. As internet revolutionized the connectivity of people, similarly IoT will transform the world into a smarter world where objects would communicate with other. To realize the full fledged vision of IoT, an efficient and secure medium is required which would ensure provisioning of reliable services. It involves sensing data ubiquitously, analyzing data and representing information through the use of cloud computing as the base. In our paper, we conceptualize IoT as day to day objects having embedded microchips within them which keep track of location of other objects as well [1]. Cloud computing is the emerging paradigm which can certainly give IoT a new direction promising ubiquitous access, improved scalability and autonomy. IoT can be thought of as a concept where we assume things as active components of business and information which are connected with each other and exchange data in the environment by using wireless sensors & RFID technology.

According to Forrester in [2] "IoT uses information and communications technologies to make the critical infrastructure components and services of a city administration, education, healthcare, public safety, real estate, transportation and utilities more aware, interactive and efficient". IoT will improve civic amenities, besides serving the industry to change the scenario of the applications in the IT sector. IoT can be thought of as a striking research field which can change the whole world through its interventions. However there exist several challenges that obstruct the efficient envisioning of the IoT to become a reality. Standardization of IoT is necessary to provide efficient services to its users.

Several researches are being made into the standardization of IoT to further strengthen the IT field. IETF has initiated the standardization to allow the objects and devices to integrate with internet services [19]. As complex technology poses several challenges, thus IETF has developed a protocol suite to meet the requirements of wireless data transmission. Further, Cisco has been working on the development and application of IPv6 protocol suite. IPv6 provides QoS, routing services, enhanced reliability and better security that will contribute immensely to the growth of IoT [20]. As IoT is an open standard, so IPv6 undoubtedly becomes the most suitable protocol accordingly. ITU-T has several active groups working on the advancement of concepts related to IoT such as its requirements, capabilities, application support models, gateway, device management and identification. ITU-T SG2 has been conducting its research focusing on numbering, naming and addressing of devices across the IoT network. Further, ITU has described data privacy and protection as among the key challenges to the growth of the Internet of Things [21].

Security is a critical issue which certainly needs to be resolved as with increasing number of users, there would be a need to handle their requests and check authenticity on the cloud based paradigm. The structure of rest of this paper is as follows: Section II discusses the challenges to the future growth of the IoT, followed by Section III which describes the general architecture of IoT and its constituent elements. Further, Section IV provides for a secure construction of IoT architecture and section V focuses on various application areas of IoT. Finally, Section VI ends up with some conclusions and future research scope in IoT security construction.

II. IOT & SMART SYSTEMS EVOLUTION CHALLENGES

Internet of Things (IoT) can certainly be termed as the biggest revolution in the making in the IT industry. The IoT will impact our living style, the way we consume energy and all our day-to-day activities. But there still exist several challenges that need to be interpreted and addressed based on the specific requirements of IoT.

A. Robustness in Connectivity

978-1-4799-6089-7/14/$31.00 ©2014 IEEE

In IoT, connecting the objects and humans through sensors and ensuring a guaranteed connectivity is an immense challenge. Also, unstable internet connectivity poses a major challenge to the IoT. Hence, there is a pressing need to work on energy harvesting devices to enhance the connectivity with the help of the energy mechanism.

B. Interoperability and Standardization

Devices manufactured by various vendors differ in technologies and services, thus making them incompatible. As all the objects would be connected through the medium of Internet, hence the task of standardization needs to be redressed to provide interoperability among the various objects and sensor nodes within the wireless sensor networks [3].

C. Naming and Identity Management

The IoT is envisioned to interconnect billions of objects across the world in various applications; therefore the need arises for unique identification of each object over the Internet. This calls for a naming and identity management scheme to be in place that is capable of dynamically assigning unique names and identities for all the objects deployed worldwide [3]. In the present scenario, shortage of address space is a major challenge which can be best resolved through the implementation of IPv6 protocol [7].

D. Safety and Security of Objects

As the IoT is built up of a large number of objects that are deployed within a defined geographic boundary, access to objects by malicious or unauthorized persons needs to be prevented to guard against their physical damage or alteration in their defined functionality [3].

E. Data Confidentiality and Encryption

As the sensor nodes carry out autonomous sensing and then transfer data to the information processing subsystem over the network, thus necessitating implementation of suitable encryption mechanisms to maintain the data integrity at the layer of information processing. Also, security mechanisms must be devised and applied to ensure the secure transfer of the transmitted data and guard against unauthorized interference or misuse of the data being transmitted across the network [3].

F. Big Data

As far as big data is concerned from the IoT perspective, we need to ensure that only relevant data is being extracted from the huge databases. The IT industry is looking forward to harness the potential of big data and the IoT can immensely contribute in gathering more information that would prove beneficial to the businesses.

III. IOT GENERAL ARCHITECTURE

Generally, the structure of Internet of Things (IoT) is divided into four layers as shown in Fig.1. The general layered architecture of the IoT and its constituent elements have been discussed:

A. Perception Layer

This layer is also known as the sensing layer. The application of intelligent sensors simplifies the connectivity among objects, besides facilitating the exchange of information amongst them. This layer consists of integrated hardware for perception and acquisition of data. Most popular sensing technologies have been discussed [1]:

1) RFID

In the paradigm of embedded communications, RFID has been a major breakthrough, thus enabling design of microchips for wireless communications. They can be embedded into objects for enabling their automatic identification. RFID tags may be passive or active. The passive RFID tags have no internal power whereas the active RFID tags are self-powered and can initiate the communication as well. The passive RFID tags are being increasingly deployed in transportation, retail, logistics, road toll tags and bank smartcards, whereas the active RFID tags find applications in auto manufacturing and remote monitoring.

2) WSN (Wireless Sensor Networks)

With the recent advancements in nano technology, wireless communications and low power integrated circuits, miniature devices are now available at much lower costs, providing much higher efficiency and also ensuring low energy consumption in remote sensing applications. This has allowed for the implementation of wireless sensor network by deploying multitude of intelligent sensor nodes, thus enabling the acquisition, processing, analysis and dissemination of useful information, collected across the network [4]. The sensed information is shared among the sensors and then sent for processing, storage and analytics.

B. Middleware Layer

This layer is interposed between the network and application layer, aiming to hide the hardware details and it allows the developers to focus on the application development process. It is responsible for providing services to the customers, besides ensuring interoperability, scalability and abstraction. Also, it authenticates the users to provide a more secure environment along with efficient delivery of services [1].

1) Data Storage and Analytics

IoT results in generation of huge volumes of data. Thus, the issues of data storage and analytics gain significance. Presently, the internet is consuming about 5% of the total energy being produced worldwide and as the IoT is envisioned to introduce billions of devices across the world, the energy consumption is sure to go up even further. Hence, it becomes pertinent to analyze the efficiency of data centers to ensure intelligent storage and usage of data for smart monitoring and actuation. A centralized infrastructure is preferred to support data storage and analytics in the IoT. Recently, cloud storage is being increasingly leveraged and in the near future, cloud

based analytics and visualization solutions are sure to give promising results [1].

2) Visualization

Visualization is another significant aspect for an IoT application which encompasses providing more information to users through a more interactive interface, thus allowing the users to interact with the surrounding environment. Recent advancements in touch screen technology have promoted the production and usage of smart tablets and phones. If the benefits of the IoT revolution are to reach the common man, focus on development of visualization that is attractive, easy to use and understand is required [1].

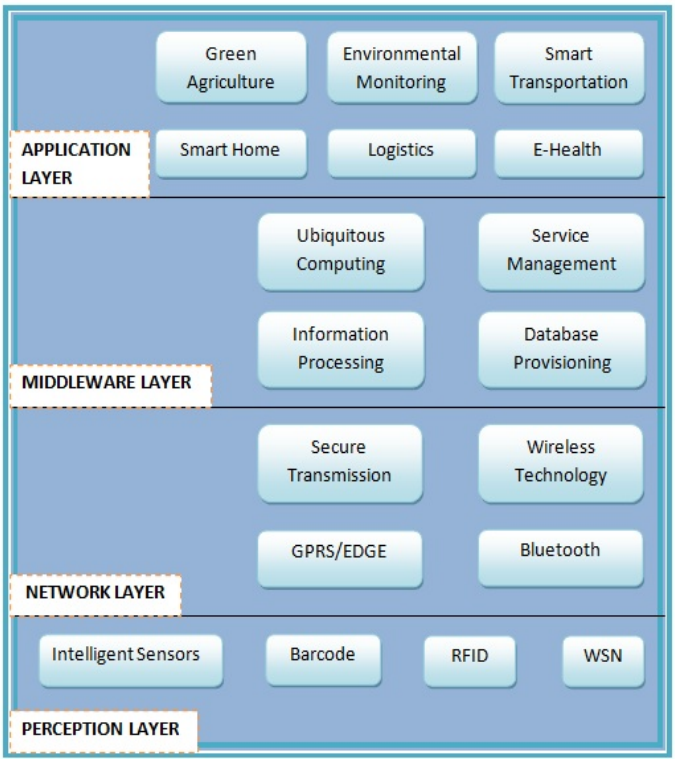

Fig 1. IoT General Architecture

C. Network Layer

The network layer provides the basic support services for secure data transfer over the sensor networks. It is also responsible for aggregating the information from various sources and routing it to correct destinations. It transfers the information over the wireless network technology such as 3G, Wifi, Bluetooth, infrared, etc [1].

1) Data Aggregation

A secure data aggregation method is required for ensuring that reliable data is being collected from sensor nodes across the network [5]. As node failures are frequent in WSNs, the network topology should be capable of healing itself. Ensuring security in the domain of data aggregation is very essential as the network is automatically connected to sensors and protection of networks from unauthorized or malicious users demands attention.

2) Addressing Schemes

In IoT, billions of objects are envisioned to be connected to each other, so it becomes necessary to provide unique identification for each of those objects. An addressing scheme that uniquely identifies objects deployed across the network is a pre-requisite to the success of IoT. The major aspects attached to a unique address include reliability, scalability and uniqueness. Presently, the IPv4 is able to uniquely identify a group of sensor devices distributed geographically, but the individual sensor devices can not be identified uniquely. Also, IPv4 faces several issues such as internet mobility issue which can be easily resolved by implementing the paradigm of IPv6. The IPv6 is capable of providing unique addresses to billions of devices. IPv6 also provides for remote access of devices along with their unique identification. A notable progress has been the formulation of a light-weight IPv6 addressing scheme that will facilitate the unique identification of household goods [6].

D. Application Layer

This is the topmost layer of the IoT architecture that provides the delivery of all the services in various fields of industry such as automobile, healthcare, education, logistics, agriculture, insurance, media, environmental monitoring etc.

IV. CONSTRUCTION OF SECURE IOT ARCHITECTURE

As compared to the existing Internet, the Internet of Things envisions to realize the communication between people and objects, objects and objects, where the focus of communication has been expanded to include objects as well [7].

In the existing Internet scenario, a plethora of protocols and technologies are available to address most of the security issues, but the existing tools have a limited applicability in the domain of Internet of Things (IoT) due to limitations on the IoT hardware nodes and wireless sensor networks. Also, the conventional security protocols consume large amounts of memory and computing resources. Another factor limiting the implementation of existing security tools is that the IoT devices usually have to work in harsh, unpredictable, and even hostile surrounding environments, where they may be prone to damage and nefarious intentions. Thus, the implementation of the existing security tools still continues to be a challenging task and hence, demands complete expertise in applied security engineering to bring in security within the Internet of Things.

Security issues corresponding to each layer of the IoT architecture need to be discussed, analyzed and resolved to the maximum possible extent [8]. Therefore, the overall security requirements of the Internet of Things encompass security of physical nodes, information acquisition security, information transmission security and information processing security, in order to achieve the authenticity, confidentiality and integrity of information [7].

A. Physical Hardware Security Policy

The perception layer forms the lowest layer of the IoT architecture and is responsible for the acquisition of information across the entire IoT network. In this layer, the foremost security issues include information acquisition security and physical security of hardware such as sensor devices, RFID nodes and sensor terminals. Due to the functional application of diverse sensor nodes having weak protection systems, predominantly in harsh surroundings, the IoT cannot implement a single security protocol and thus lack of proper security arrangements affect the security of RFID sensor nodes, wireless sensor networks, routers and sensor terminals [7]. The physical security implementation at the perception layer must provide for the physical security of the sensing hardware such as RFID nodes, sensor network and sensor terminals.

1) RFID Security Policy

As majority of RFID sensor nodes are deployed in harsh environments, hence they remain vulnerable to damage or theft and policies must be designed and implemented for replacement of damaged nodes across the wireless sensor network. The security issues related to RFID include leakage of location information of RFID tags and users, replay attacks, man-in-the-middle attacks, cloning attacks and tampering. Trade-off between cost and security needs to be balanced and suitable security policies must be designed for the RFID applications.

The RFID security is mainly implemented through the physical methods or code mechanisms or a combination of both the methods. Several categories of the physical methods have been discussed [9]:

a) Data encryption: Encryption algorithms can be applied to ensure the security of the RFID tag information.
b) Blocker tag: These tags can be used to conceal the serial number of other RFID tags by emitting a constant frequency of fake tag serial number [10].
c) Tag frequency modification: Frequency spectrum of the tags can be modified to make it difficult for malicious users to access the communication between RFID tags and readers.
d) Jamming: Radio signals can be used to jam the operations of nearby RFID readers.
e) Kill order policy: Under this policy, the tags are physically destroyed.

The RFID security issues can also be resolved through implementation of code mechanisms. These code mechanisms involve the design of protocols that tend to resolve the security issues related to RFID nodes. Some of the RFID security protocols are Hash Lock protocol, LCAP protocol, Hash chain protocol, re-encryption protocol, etc. [11-13]

2) Sensor Network Security Policy

The security contentions related to sensor network technology include physical capture of sensor nodes and gateway nodes, integrity attacks, congestion attacks, DOS attacks and node replication attacks. RFID tags differ from sensor nodes in that the RFID tags relate to static properties of things whereas the sensors relate to dynamic properties of things [14]. Construction of security framework for the sensor network involves integration of several security policies such as encryption algorithms, key distribution policies, intrusion detection mechanisms and security routing policies [15]. Some of the existing security frameworks are TinySec, LEAP protocol, parameterized frequency hopping, etc.

a) Key distribution policies: Usually, the sensor networks opt for random key pre- distribution where each of the sensor nodes randomly chooses few keys from the pool of available keys such that each set of two nodes are able to share keys with higher probability.
b) Intrusion detection mechanisms: These mechanisms provide an additional layer of security in the Internet of Things as they timely discover the security flaws in the networks and hence appropriate security remedies can be provided [15, 17-18].
c) Security routing policies: Security routers can be deployed across the network to enhance its security. Some of the most widely used security routing policies include multi-path routing policy may be adopted to guard against forwarding attacks. Also, flooding attacks need to be dealt with by restricting the routing of nodes to a particular range [16].

3) Sensor Terminals Security Policy

Security issues related to the terminals of sensors in the Internet of Things include unauthorized access, theft or damage of confidential information, duplication of SIM information, access and imitation of air interface information, etc. Data is sensed through multiple sensor nodes, after which it is transmitted to the data processing subsystem and then it finally reaches intended users and applications. Widely deployed sensor terminals include smart phone, personal computer, laptop, tablet, etc. Most commonly used security policies for sensor terminals include cryptographic algorithms, identity authentication policies, data flow control policies, data filtering mechanisms, etc [7].

B. Information Acquisition Security Policy

Besides the physical security issues, the perception layer also need to tackle issues related to information acquisition security. Information acquisition security issues include wiretapping, tampering, cheating and replay attacks. Security policies related to data acquisition have been discussed:

- Authenticity, confidentiality and integrity of data must be ensured during the phase of data acquisition;
- The key management protocol in the perception layer needs to be strengthened, including the application of lightweight symmetric and asymmetric key management policies;
- Secure routing policies must be adopted to ensure authentic route discovery and effective network security.
- Sensor node authentication policies must be leveraged to prevent data access by unauthorized and malicious users [8].

C. Information Processing Security Policy

In the IoT architecture, the middleware layer is mainly responsible for information processing and it also provides communication interface between the network and application layers of the IoT layered architecture. The security implementation at the middleware layer needs to ensure confidentiality and safe storage of information as well as safety of middleware. There still exist several technical issues related to the reliability, privacy and security of information processing in the middleware layer of IoT architecture [7]. The application layer may provide various applications such as green agriculture, smart house, smart transportation, etc. and the major security issues the application systems are facing include malicious programs and design flaws.

D. Information Transmission Security Policy

In the IoT architecture, the prime responsibility of network layer is transmission of information across the network. The IoT architecture, being implemented on the basic communication framework, remains prone to its associated risks such as denial of service attacks, unauthorized access, man-in-the-middle attacks, virus attacks in addition to compromise on confidentiality and integrity of data. As the IoT involves sensing and acquisition of data from a multitude of devices, with data being collected in various data formats; the collected data acquires a heterogeneous character, and this brings in other complex network-related issues such as large number of nodes transferring data leading to network congestion.

The security strategies at the network layer need to maintain the authenticity, confidentiality, integrity and availability of the data while it is being transmitted across the network. The IoT applications involve the transfer of large amounts of data across the IoT network and this necessitates the application of various authentication, filtering and detection mechanism to ensure security of data. The data must also be guarded against DDOS attacks by implementing DDOS attack detection and prevention. Also, the heterogeneous nature of network connection results in information exchange vulnerabilities, replay attacks, etc. Authentication mechanisms, key management and negotiation mechanisms, and intrusion detection mechanisms can be leveraged to make the network immune against such attacks [8].

E. Information Application Security Policy

As the application layer of the IoT architecture deals with huge amounts of data, the applications face several data security issues as well as data privacy issues. Data protection, data backup and recovery mechanisms must be in place to achieve data security. To ensure data security at application layer, data security management and encryption/decryption algorithms must be applied to secure the database. Access management mechanisms to prevent unauthorized access to the database and management of database administrative privileges, both strategies can be implemented for securing the database.

Another component of security implementation at the application layer level is privacy of data. In many IoT applications, data privacy protection assumes significance. The term data privacy suggests that the data owners do not want their sensitive data set to be disclosed to unauthorized access. To prevent unauthorized access and usage of the data, access privileges must be limited and the data related operations must be based as per the level of security or access rights. Data distortion technology, data encryption technology or privacy agents are some of the technologies upon whom the common privacy protection technologies may be based upon for ensuring privacy of the database.

Peer-to-peer computing and semantic web are two major privacy protection strategies. Peer-to-peer computing enables the peer computer nodes to share their services and computing resources among each other whereas semantic web defines and organizes information through specific standards in order to make the semantic information more clear and understandable to the machines and to implement human-machine communication [17]. Various other data privacy techniques include virtual private network, TLS, SSL, DNS security extensions and location privacy protection [18].

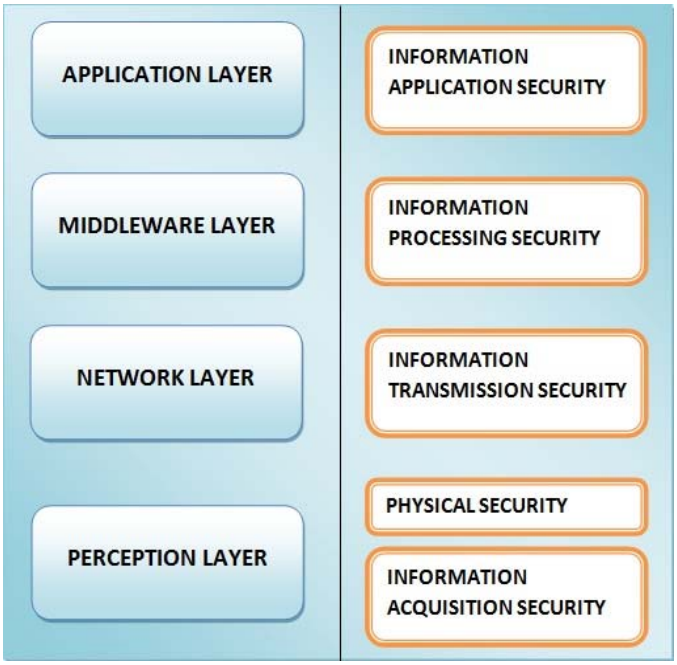

Fig 2. Construction of Secure IoT Architecture

V. APPLICATIONS OF IOT

TABLE 1: APPLICATIONS OF IOT

Field of Application	Examples of Application
E-Health	Patient monitoring, Doctor tracking, Personnel tracking, Real-time patient health status monitoring, Predictive expertise information to assist doctors and practitioners.
Retail & Logistics	Supply Chain Control, Intelligent Shopping Applications, Smart Product Management, Item Tracking, Fleet Tracking.
Smart Transportation	Smart transportation through real-time dynamic on-demand traffic information and shortest-time travel path optimization.

Energy Conservation	Smart Devices, Smart Grid.
Smart Home	Energy Use, Water Use, Remote Control Applications, Intrusion Detection Systems.
Environmental Monitoring	Air Pollution, Noise Monitoring, Waterways, Industry Monitoring.
Green Agriculture	Green Houses, Compost, Irrigation Management, Soil Moisture Management.

VI. CONCLUSION

The world has begun witnessing the impact, the Internet of Things is making on various application fields by realizing the maximum potential of Internet. The technologies being leveraged in the IoT certainly need to overcome the challenges posed to their practical implementation. Rapid advancements in the IoT have led to the emergence of security construction in the IoT architecture as an important subject. Although, researches are being conducted into the security implementation of the IoT, but still several security aspects need much deeper introspection.

In this paper, security issues in each layer of the IoT architecture have been analyzed and appropriate strategies have been suggested, which can certainly be improved with future technological prowess, for secure construction of IoT architecture. Also, the challenges to the successful realization of the IoT such as naming and identity management, standardization have been discussed. Future researches in the security issues of IoT must focus on physical hardware security, privacy of information being collected, processed and transmitted across the network. Besides appropriate technical strategies, realization of secure IoT also calls for a series of policies, laws and regulations to strengthen the security system.

REFERENCES

[1] 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, no. 7, pp. 1645-1660, ISSN: 0167-739X, Elsevier Science, Amsterdam, The Netherlands, 2013.

[2] J. Belissent, “Getting Clever About Smart Cities: New Opportunities Require New Business Models,” Forrester Research, 2010.

[3] R. Khan, S.U. Khan, R. Zaheer and S. Khan, “Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges” in Proceedings of the 10th International Conference on Frontiers of Information Technology, December 17-19, 2012, pp. 257-260.

[4] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “Wireless Sensor Networks: A Survey,” Computer Networks 38, 2002, pp. 393–422.

[5] Y. Sang, H. Shen, Y. Inoguchi, Y. Tan and N. Xiong, ”Secure Data Aggregation in Wireless Sensor Networks: A Survey,” 2006, pp. 315–320.

[6] M. Zorzi, A. Gluhak, S. Lange and A. Bassi, “From Today’s Intranet of Things to a Future Internet of Things: A Wireless- and Mobility-Related View,” IEEE Wireless Communications 17, 2010, pp. 43–51.

[7] L. Li, “Study on Security Architecture in the Internet of Things,” International Conference on Measurement, Information and Control (MIC), 2012, vol. 1, May 18-20, pp. 374-377.

[8] Q. Gou, L. Yan, Y. Liu and Y. Li, “Construction and Strategies in IoT Security System,” IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Aug 20-23, 2013, pp. 1129-1132.

[9] E. Korkmaz and A. Ustundag, “Standards, Security & Privacy Issues about Radio Frequency Identification (RFID),” RFID Eurasia, 2007 1st Annual, pp. 1-10, DOI: 10.1109/RFIDEURASIA.2007.4368148.

[10] Y. Ping, “Privacy Security in Mobile RFID Networks,” Journal of Chongqing College of Electronic Engineering, 2010, vol. 19, pp. 91-92.

[11] O. Savry and F. Vacherand, “Security and Privacy Protection of Contactless Devices,” The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications, New York: Springer New York, 2010, pp. 409-418.

[12] B.F. Bian and O. Gunther, “Security Challenges of the EPC Global Network,” Communications of the ACM, 2009, vol. 52, no. 7, pp. 121-125.

[13] Z. Yong-Bin and F. Deng-Guo, “Design and Analysis of Cryptographic Protocols for RFID,” Chinese Journal of Computers, 2006, pp. 583-584.

[14] Z. Fu-Sheng, “Internet of Things: Open a New Life of Intelligent Era,” Shan Xi People's Publishing House, 2010, pp. 175-184.

[15] L. Xiao-Wei, “Wireless Sensor Network Technology,” Beijing Institute of Technology Press, 2007, pp. 241-246.

[16] W.Y. Chao, W. Wei and L.D. Mingo, “Summary of Wireless sensor network security Computer Era,” 2008, vol. 12, pp. 15-19.

[17] D. Leusse, P. Periorellis and P. Dimitrakos, “Self Managed Security Cell, a Security Model for the Internet of Things and Services Advances in Future Internet,” First International Conference on Digital Object Identifier, 2009, pp. 47-52.

[18] V. Oleshchuk, “Internet of Things and Privacy Preserving Technologies,” First International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronics Systems Technology, Aalborg, 2009, pp. 336-340.

[19] Z. Sheng, S. Yang, Yifan Yu and A. Vasilakos, “A Survey on the IETF Protocol Suite for the Internet of Things: Standards, Challenges, and Opportunities,” vol. 20, no. 6, pp. 91-98, ISSN: 1536-1284, Wireless Communications, IEEE , 2014.

[20] “The Internet of Things How the Next Evolution of the Internet is Changing Everything,” Cisco Internet Business Solutions Group (IBSG), April 2011.

[21] B. Jamoussi, “IoT Prospects of Worldwide Development and Current Global Circumstances,” October 28-30, 2010. Available: http://itu.int/ITU-T/go/IoT