I J C T A, 9(41) 2016, pp. 743-752 ISSN: 0974-5572

SECURITY IN INTERNET OF THINGS

Anurag Shukla and Dr. Sarsij Tripathi

Abstract: The Internet of Things (IoT) is the next Era of innovation that promises to enhance and improve our daily life based on smart sensors, internet and objects working together. By Internet Protocol (IP) connectivity, devices can now be communicated to the Internet, thus allowing them to be sense, managed and controlled and at any time and at anywhere. Security is a key point for IoT deployments. In this survey paper, we study the security methods of Internet of things (IoT). Typically, IoT architecture has been divided into three layer Perception or sensing layers, Network and Application layers. Many security principles that should be at each layer are also presented. We investigate how existing security methods for internet communication ensure major security requirements with respect to IoT, together with possible IoT research challenges.

Key Words: *Internet of Things, IoT Elements, Security Architecture, privacy, security and IoT challenges.*

I. INTRODUCTION

The term IoT, is a combination of uniquely identifiable things, heterogeneous objects, and there representation on internet –structure, was firstly introduce in 1998 [1]. Now days, IoT is gaining popularity through some useful application (Energy monitoring system, e-Health care and smart transportation system). Generally, IoT has five basic components: identification, sensing, communication between device, data processing, applications and services, and need to provide secondary components such as privacy and security.

As concern to security, the IoT is facing more critical challenges. Hence, these are the following reasons: I) the IoT expend the 'internet' by the mobile network, sensor and internet so on, II.) Each object will be virtually available on this 'internet', and III) All these 'different things' will interact or communicate to each other. Hence, the new security threads and privacy problems will emerge. We must pay more observation to find the possible research issues for ensure integrity, authenticity and confidentiality.

II. IOT ELEMENTES

2.1. Idetification –

In IoT, Identification is an important part for naming the object and map there offer service. Many techniques are introduced for identification purpose in IoT, ubiquitous codes (uCode) and electronic product codes (EPC) one of them [2]. With respect of IoT objects, it is difficult to distinguish between address and object ID. Object ID can be a name such as "E1" for a specific energy sensor and Object's address is an address within a particular network. Some of the addressing techniques for IoT objects are 6LoWPAN, IPv4 and IPv6 and. 6LoWPAN offers a compression technique in IPv6 headers that make it useful for low power wireless networks [3], [4]. Identification and object's address both are essential, since identification methods useful in case of object identification in case of local network not globally. When object with in communication network, there can be a possibility to use public IP not the private one. Identification techniques can be utilized to allocate a uniquely indentify for every object within the network.

Department of Computer Science and Engineering, NIT Raipur, Raipur, Chhattisgarh, India
Emails-anurag672@yahoo.com , stripathi.cse@nitr.ac.in

2.2. Sensing –

In IoT, sensing is collect information from applied sensors or nodes within the network and transmitting it to a database, cloud or data warehouse. The gathered information is examined to predict appropriate action based on needed services. The IoT sensors can be wearable devices, intelligent sensors and actuators so on. For example, Bosch, Zonoff , Smart Things (companies) provide services to user so they can operate number of smart devices in building through mobile application in his/her phone [5].

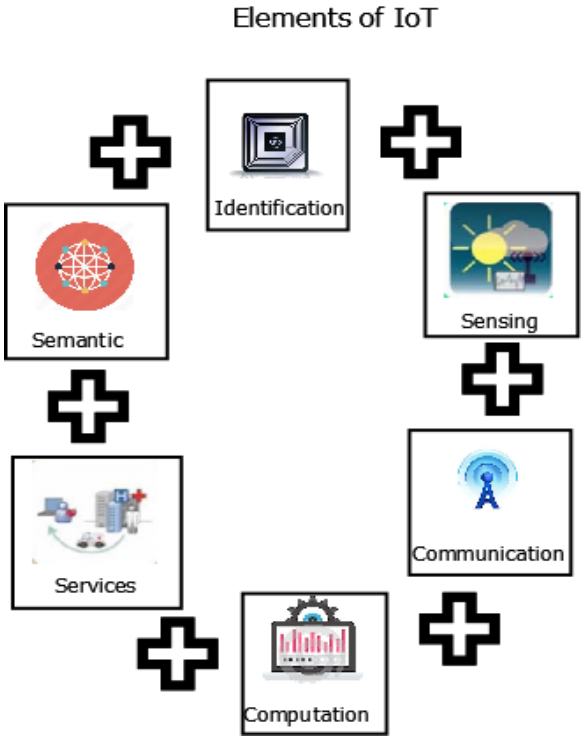

Figure 1. THE IoT ELEMENTS

2.3. Communication –

In IoT, variety of objects together by communication network to provide some appropriate services. Generally the IoT device should run at less power in the presence of reliable or unreliable network (lossy and noisy). Some of the protocol for IoT communication techniques is LTE-Advanced, WI-Fi, Bluetooth and Z-wave. Some communication techniques are also applied like RFID and Near Field Communication (NFC). RFID (tag and reader) is known as the first technology used to achieve the Machine-to-Machine (M2M) communication. The RFID tag is a small chip used to trace the object. The RFID reader sends a request to RFID tag and gets response, which is send to the cloud or database. The cloud or database is in contact with the computation center to trace objects through the receive signal. There are basically two categories of RFID: active and passive. Active tags need a battery power while passive not. 6].

The NFC is 2- way interactions between devices. The NFC protocol can transmit data from 100 to 424 kbps, frequency band at 13.56MHz and, range in between 20 cm where communication between objects[7]. The Ultra-wideband (known as UWB or ultra-wide band and ultra band) is a radio technology that can run on very low energy level for short-range and support high-bandwidth communications over sensors communication [8].

LTE (Long-Term Evolution) provides high data transfer scheme for devices based on UMTS/GSM. It is a wireless communication technique and provides broadcasting and multicast service as well. LTE

Advanced is an advance form of LTE, which offer bandwidth up to 100 MHz, lower latencies and higher throughput [9] [10]. Another communication technology offer device communication and data sharing without using any router in ad-hoc manner. Wi-Fi works on radio waves to data range up to 100 m [11]. Bluetooth can operate on low power and exchange data up to 150m by using short-wavelength radio [12].

2.4. Computation –

Microcontroller or microprocessor and some software unit represent as mind of "IoT" and have computational ability. Various hardware platforms are introduced for support IoT application such as Arduino, Raspberry Pi and so on.

Also, number of software platforms is used to offer IoT services. Among all, OS (Operating Systems) are crucial and they use all time since activation of an object. In IoT, There are many Real-Time Operating Systems (RTOS), where real time base application of iot can be simulate easily. For example, the Contiki RTOS is used mostly in IoT applications. Contiki has a simulator known as Cooja offer environment in which user can simulate IoT and WSN applications [13].

Cloud Platforms is one of the useful parts of the IoT. Smart device can store their sense information to cloud or and collected information to be analyzed (real-time) and application users will get advantage from the store data. There are a lot of low cost and pay as a service cloud platforms available to host IoT services.

Table -1 Basic Blocks And Technology of IoT

IoT Elements		Support
Identification	Addressing	IPV4, IPV6
	Naming	EPC, uCODE
Sensing		Wearable Sensor, RFID Tag, Acurator
Communication		WiFi, Bluetooth, IEEE 802.15.4,RFID, Thread,NFC, UWB,Neul
Computation	Software	OS(Tiny OS, Contiki)
	Hardware	Arduino, Raspbeery Pi Clouds(Hadoop etc)
Service		Energy Monitoring System, Smart Home, e-Health Care and Smart City etc.
Semantic		RDF,OWL,EXI

2.5. Services –

Overall, IoT services can be classified in 4 classes [23], [24]: Collaborative Aware Services, Identity-related Services, Information Collection, and Ubiquitous Services. Identity related services are most fundamental and necessary that is used in various types of applications. Each application requires an involvement in between real object, virtual world and has to maintain unique identity. Sensing-data collection aggregates and summarizes raw data need to be processed in real time and store on the database

or cloud. Collaborative-Aware Services work together with Information Aggregation and examine the collected data to identify the next decision and response accordingly. Ubiquitous Services make available Collaborative-Aware Services when they are required to any person at any place. At the end the main conclusion is IoT application should reach the level pervasive service and this will not be easy still many challenges that need to be covered. Some of the standard applications offer information collection, identity related services and collaborative-aware services. E- Monitoring healthcare system and smart grids come into the information collection category and smart city, smart transportation systems (STS), energy monitoring and industrial automation come under the collaborative-aware category.

2.6. Semantic –

In IoT, Semantic means the ability to gather knowledge smartly from different machines to offer the request services. Also, it includes how the data is analyzing so that make sense of the correct decision to match exact the demand service [13]. Hence, semantic can be call as "mind" of the IoT by balancing needs to the required resource. This entire need is provided by Semantic Web techniques such as the Web Ontology language (OWL) and the Resource Description Framework (RDF). World Wide Web (www) in 2011 selects the Efficient XML Interchange (EXI) format as a suggestion [14].

EXI is precious with respect to the IoT because it is introduced to improve for resource-constrained environments in XML applications. It decrease bandwidth requirement without disturbing any resources such as memory size, energy computing and battery life. EXI transforms XML format messages to binary code and decease the required bandwidth and minimize the needed memory size.

In this discussion, we cover the basic element of the iot and required common technology for each section. For heterogeneous object it is complex to implement and make ubiquitous for IoT service. In the next section we cover the possible security architecture for IoT and try to address, number of possible security threads for each section.

III. IoT Security Architecture and features

Different industry is requiring different IoT application standard and there specifications. Common IoT architecture has not introduced yet. Many organizations have released security standards of IoT such as ETSI, IEEE etc. Article [15] suggests that there is need of various security standards. Many of traditional IoT solutions are independent to the small networks; some of them can be hacked. With the continuous development of IoT, the small networks will bind and make a large network then; it will be more challenging to maintain the security. With the IoT development, by binding small impendent network will make a large network then, it can cause new security problem. This security will be very crucial in development of IoT.

3.1. IoT Security Architecture –

Generally, IoT architecture divides into 3 layers-perception, network, and application layer [16]. Support layer (such as cloud computing, intelligent computing) also include in some system as the support for application layer [17]. In this survey paper we will consider three layer architectures. “Fig. 2” provides the architecture view of IoT security.

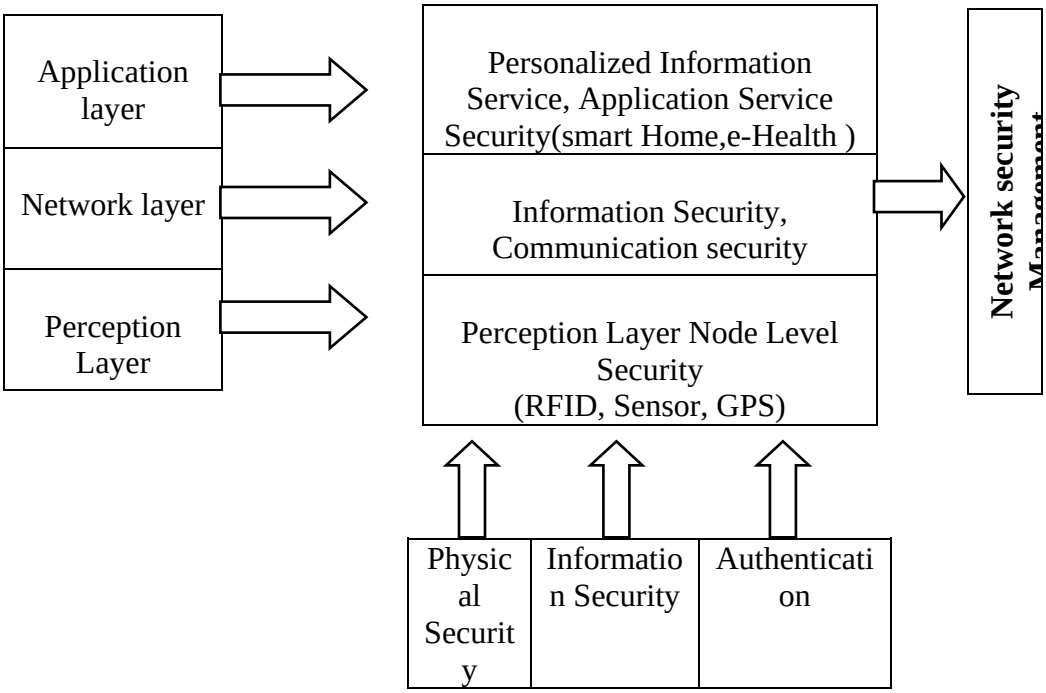

Figure 2. Security Architecture

3.2. IoT and Security Features–

IoT should cover three characteristics: inclusive perception, reliable communication, and smart computation. Inclusive perception means perception layer sensor gather information of object or environment attribute at anytime and from anyplace reliable communication means that unmodified attribute value of object while communication is achieve by the wired or wireless network to the database or cloud in real time, smart commutation means before submitting to application terminal, arranging the gather information and make analysis.

IoT features must consider the nature of IoT security. In the following section, first three are standard security features, and rest of the current features [16] [18]:

3.2.1. The Security Problems in Data Collection and Transmission at Perception Layer –

Sensor nodes have many diversity in terms of processing power (Low) and energy. So, these make them could not get high complex security techniques.

3.2.2. The classical Network Layer Security Issues –

Security architecture for internet is very mature with respect of various technology, there are still many attack can be happen. For example, at a same time large number of objects send data; result in DoS attack.

3.2.3. The Security Problems at Application Layer–

In different application, there are various security problems. For example: Authentication, privacy protection etc.

3.2.4. Relationship between Security and Cost –

In the network, if large number of node cost is low, then due to this security of network will be decrease. On the other hand, at high-performance nodes could be more secure, but network maintenance will be increase.

3.2.5. Lightweight –

The sensor node has low processing power, so there must be low light weight secure algorithm (Encryption and Authentication).

3.2.6. Complexity –

Different applications have different type of security problems and. So level of security maintain at each layer accordingly.

IV. THE INTERNET OF THINGS SECURITY PROBLEMS

As concern to security, IoT will be facing more serious challenges. These are some possible reasons: 1) the IoT expands 'internet domain' by the traditional internet, sensor network and mobile network 2) every 'object' will be connected to the 'internet', and 3) these 'object' will communicate with each other from any place, anywhere. So there will be a possibility of new security and privacy problems will arise, which is given below.

4.1. Security Problems At Perception Layer–

All types of sensors: (GPS, zigbee and RFID) is the main thing in perception layer. When these sensors sense the data, sensed data is transmitted by the wireless network (mostly). If it lacks secure, signals can reveal, leak, interrupted easily. The most of sensor are set up on the anonymous place, so there is a chance attackers can easily reach to the sensor location and, harm physically or control them.

Table -2 Specification of IoT Layer

Layer	Component	Service	Security Issues	Security Parameter
Perception layer	Smart Card, RFID tag, Sensors	Information Collection	Physical Security issue Sensor network security issue	Authentication, Confidentiality
Network layer	Wireless or Wired network Routing	Information Transmission	Communication security	Integrity, Availability, Confidentiality
Application layer	Intelligent devices	Analysis of information, decision making	Information processing safety of IoT	Privacy

Some common attack given below [15] [19]

- Key nodes like gateways are controlled easily by the malicious person. It may reveals all precious data, like secret key of data encryption and matching key etc and breach the security of entire network.
- The attackers can introduce a fake node in the network, and input dummy information. They try to disturb communicate information. The sleeptime of the limited energy node is disturbed and consumes more energy. So, it will be wastage of resource and will disturb the entire network.
- DoS is most popular attack in communication network. It makes service and resources unavailable.
- By estimating the encryption algorithm execution time, can predict key information.

4.2. Network Layer Security Problems–

- Classical Security Issues: In network communication, common security problems are integrity and data confidentiality. Even if the traditional communication protocol has cover some security issues, but, there are still some security issues, including eavesdropping data damage, illegal access, exploit attacks, confidentiality, DoS attack, integrity damage, virus infraction, , etc.
- Compatibility problems. The traditional Internet securities techniques are planed with respect of person, not for things. Using the traditional security techniques will divide the logical relationship between IoT things. Heterogeneity makes security, coordination and interoperability of network becoming worse.
- DoS attack, network congestion, and authentication problem are categories under cluster security Problems. Iot is a collection of many devices if it follows the traditional authentication method, this make mutual authentication among lot of ioT equipment. Hence, huge amount of data traffic will generate from these devices and likely to block the whole network and make resource unavailable. So, it is a waste of the high cost resources.

4.3.Application Layer Security Problems–

- In IoT, Variety of applications can have different strength of application users. So in order to control illegal accesses, there is requirement of productive authentication technique. Identification of irrelevant and malicious data should also be considered.
- When a programmer writing software, there is a possibility of writing nonstandard codes. It can cause memory overflow. Hacker can use this point and can crash the entire system.
- Because of a many number of users, huge data is transmitted at communication link, once the data computing strength cannot match the needed requirements, it can cause to network congestion.

V. THE INTERNET OF THINGS SECURITY MEASURES

In IoT sensor networks, heterogeneity in object and network make security more complicated. This section will give study about security mapping technology involved at perception, network and application layer.

5.1. Security Measures In Perception Layer–

In perception layer of IoT, RFID and WSN are main part. Their security measure covers respectively in below section.

5.1.1. Security Measures Of RFID [22]–

A. Access Control–

Main to focus on user's privacy and try to make secure the sense data of RFID tags cannot be read by third party. In these, including node failure, energy analysis and chip protection etc.

B. Data Encryption–

To maintain security of RFID information there is a need an encryption mechanism to encrypt the data through the specific light weight algorithm. To maintain the high-speed communication, this algorithm should use less computing power, and maintain high security.

C. IPSec Security–

IPSec offers 2 levels of security techniques: encryption and authentication. In IP communication, the receiver is ensured the validation the sender identity by authentication technique. Data encryption techniques can block hacker from eavesdropping and information breach while communication and encode data for make sure the data is confidential.

D. Cryptography Techniques–
Cryptography methods assure the user privacy protection as well as take care of the integrity, authenticity and confidentiality of RFID data. Communication security techniques use the concept of random numbers technique, the logic algorithm, the hash function, and re-encryption mechanism.

5.1.2.WSN Security Measures [22]–

A. Key Management–
There are 4 key distribute protocols: pre distribution scheme, simple key distribution scheme, and hierarchical key and dynamic key management protocol.

B. Secure Key Algorithms–
Asymmetric keys algorithm apply Rivest Shamir Adleman and Elliptic Curves Cryptography techniques. Symmetric key algorithms apply Skipjack and RC5. Perceptual nodes have less computation power. Therefore, symmetric key algorithms(less computation cost) are mostly used in WSN.

C. Intrusion Detection Technology –
IDS can observe the behavior of network nodes time to time, and find the unsure behavior of nodes.

5.2. Security Measures In Network Layer–

In the current scenario of IoT, network layer security techniques based on based on the internet protocol communication. But the existing security techniques are not fulfilling the complete requirements with respect of IoT. Because of IoT sensor arrange randomly, autonomist and imitated in terms of energy, it leads to dynamic infrastructure. So, the attacker can easily break the application security.

For variety of IoT application, we need to apply the appropriate authentication technique and key techniques, for wireless WPKI, PKI etc.

5.3. Security Measures In Application Layer–

A. The Saftety of the Private Information–
It includes anonymous authentication, digital watermarking and Biosecurity etc.

B Increasing the Awareness of Safety –
Application users need to understand the value of security and how to use correctly in IoT offer applications. Therefore, leakage of confidential data is reduce.

VI. CHALLENGES IN INTERNET OF THINGS

The IoT offers many new application and services to the automation industry. Still yet, in IoT requires common protocol, techniques, architecture that integrate the virtual world and real world in one framework [20] [21]. Some of the following challenges are listed below.

6.1 Architecture Challenge –

IoT involves increasingly number of heterogeneous devices and sensor. As the communication can be take place in these devices and at anyplace and at anytime for any require service. This communication is achieved in wireless and ad hoc manner. In IoT, data generates from different devices and services require infrastructure support to integrate the generated information from many objects and identify applicable attributes, to analysis gathered data and highlight their possible relation, and predict future decision. Common static architecture cannot be a blueprint for variety of services. Therefore, dynamic architecture which can support for several of object and application need to be introduce in IoT.

6.2.Privacy and Security Challenge –

Comparison with classical networks, privacy and security relate threads of IoT become much more important [22]. Most of the information is about the user privacy only, so that privacy protection an important security issues in IoT. Traditional security architecture is proposed with respect of H2H (Human to Human) communication, may not be applicable for IoT system. Using existed security methods will not provide support to IoT object. IoT needs low computation & less energy-cost with respect of M2M (Machine 2 Machine) solutions, who assure the the privacy and the security. Related research should be focus on privacy.

6.3 Standard Challenge –

In IoT, standard is an important part. A standard gives opportunity to objects to use and access the resource equally. Balancing a ratio in between standards and proposals will gain efficient growth of IoT infrastructures and services applications. The standard development process and protocol should be open accesses to all, so that when new devices will introduce in network, existing standard can be modified to support new object and application. In today's network paradigm, global standards are typically more applicable than any local agreements.

VII. CONCLUSION

The development of security is a key part of IoT. In this paper we exposes many security problems at each layer of IoT and there possible solution. But IoT as a large system is collaboration of several layers and continuously increasing, and large number of security problem come from System collaboration so that there are still some of the security problems not residing to any specific layer at a time, which is need to be cover in future.

In this survey, we covered basic IoT elements and require support technology for each element, security architecture of IoT support. We focus on possible privacy and security concern at different layers in IoTs. Additionally, we identified many open issues related to the privacy and security that is not covered by existing standard security technique so; need to be focused by researcher and research community to make a trusted platform for the delivery of future IoT. We also address some of IoT challenges. In future, IoT will remain a hot issue for the research.

REFERENCES

[1] R. H. Weber, "Internet of things – new security and privacy challenges," Computer Law & Security Review, vol. 26, pp. 23-30, 2010.

[2] N. Koshizuka and K. Sakamura, "Ubiquitous ID: Standards for Ubiquitous computing and the Internet of Things," IEEE Pervasive Comput., vol. 9, no. 4, pp. 98–101, Oct.–Dec. 2010.

[3] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over Low Power Wireless Personal Area Networks (6LoWPANs): Overview, assumptions, problem statement, and goals," Internet Eng. Task Force (IETF), Fremont, CA, USA, RFC4919, vol. 10, Aug. 2007.

[4] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 packets over IEEE 802.15. 4 networks," Internet Eng. Task Force (IETF), Fremont, CA, USA, Internet Proposed Std. RFC 4944, 2007.

[5] U. Rushden, Belkin Brings Your Home to Your Fingertips With WeMo Home Automation System. Los Angeles, CA, USA: Press Room Belkin, 2012.

[6] Technical report by N.Srivastava on RFID: RFID Introduction, Present and Future applications and Security Implications, George Mason University, Fairfax, VA, Fall, 2006.

[7] R.Want, "Near field communication," IEEE Pervasive Comput., vol. 10, no. 3, pp. 4–7, Jul./Sep. 2011.

[8] R. S. Kshetrimayum, "An introduction to UWB communication systems," IEEE Potentials, vol. 28, no. 2, pp. 9–13, Mar./Apr. 2009.

[9] G. V. Crosby and F. Vafa, "Wireless sensor networks and LTE-A network convergence," in Proc. IEEE 38th Conf. LCN, 2013, pp. 731–734.

[10] A. Ghosh, R. Ratasuk, B. Mondal, N. Mangalvedhe, and T. Thomas, "LTE-Advanced: Next-generation wireless broadband technology [Invited Paper]," IEEE Wireless Commun., vol. 17, no. 3, pp. 10–22, Jun. 2010.P. Kumswat, Ki.

Attakitmongcol and A. Striaew, "A New Approach for Optimization in Image Watermarking by Using Genetic Algorithms", *IEEE Transactions on Signal Processing*, Vol. 53, No. 12, pp. 4707-4719, December, 2005.

[11] E. Ferro and F. Potorti, “Bluetooth and Wi-Fi wireless protocols: A survey and a comparison,” IEEE Wireless Commun., vol. 12, no. 1, pp. 12–26, Feb. 2005.

[12] A. Dunkels, B. Gronvall, and T. Voigt, “Contiki—A lightweight and flexible operating system for tiny networked sensors,” in Proc. 29th Annu. IEEE Int. Conf. Local Comput. Netw., 2004, pp. 455–462.

[13] P. Barnaghi, W. Wang, C. Henson, and K. Taylor, “Semantics for the Internet of Things: Early progress and back to the future,” Proc. IJSWIS, vol. 8, no. 1, pp. 1–21, Jan. 2012.

[14] T. Kamiya and J. Schneider, “Efficient XML Interchange (EXI) Format 1.0,” World Wide Web Consortium, Cambridge, MA, USA, Recommend. REC-Exi-20110310, 2011.

[15] Mengmeng Sun, Yuan’an Liu, Kaiming Liu. : Security problem analysis and Security mechanism research in IoT. J. Secrecy Science and Technology Nov.2011.

[16] Kai Zhao,LinaGe"A Survey on the Internet of Things Security" IEEE 9th Int. Confr. on Computational Intelligence and Security,2013.

[17] H.Suoa, J. Wana,C. Zoua, J. Liua"A Survey on the Internet of Things Security" IEEE Int. Confr. on Computer Science and Electronics Engineering,2012.

[18] Jianhua Sun, Changxiang Chen, “ Initial Study on IoT Security. J. Communications Technology”. 45(7) 2012.

[19] Shancang Li, Kewang Zhang. :” Principle and application of wireless sensor network”. M. Beijing: China Machine Press 2008.

[20] R. Kranenburg and A. Bassi, “IoT challenges,” Commun. Mobile Comput., vol. 1, no. 1, pp. 1–5, 2012.

[21] S. Chen,H. Xu, D. Liu,B. Hu, and H. Wang “A Vision of IoT: Applications, Challenges, and Opportunities With China Perspective,” Commun. Mobile Comput., vol. 1, no. 4, pp. 349–358, 2014.

[22] Lei Li, Jing Chen. "System Security Solutions of RFID System ofInternet of Things Sensing Layer" J. Net Security Technologies and Application, vol.6, PP.34-36,2011.

[23] X. Xiaojiang, W. Jianli, and L. Mingdong, “Services and key technologies of the Internet of Things,” ZTE Commun., Shenzhen, China, vol. 2, p. 011, 2010.

[24] M. Gigli and S. Koo, “Internet of Things: Services and applications categorization,” Adv. Internet Things, vol. 1, no. 2, pp. 27–31, Jul. 2011.