A Critical Analysis on the Security Concerns of Internet of Things (IoT)

M.U. Farooq
Electronic Engg. Dept.
PAF-Karachi Institute of Economics and Technology, Pakistan

Muhammad Waseem
Telecommunication Engg. Dept.
Sir Syed University of Engg. and Technology, Pakistan

Anjum Khairi
Electronic Engg. Dept.
Sir Syed University of Engg. and Technology, Pakistan

Sadia Mazhar
Electrical Engg. Dept.
Sir Syed University of, Engg. and Technology, Pakistan

ABSTRACT

Internet of Things (IoT) has been a major research topic for almost a decade now, where physical objects would be interconnected as a result of convergence of various existing technologies. IoT is rapidly developing; however there are uncertainties about its security and privacy which could affect its sustainable development. This paper analyzes the security issues and challenges and provides a well defined security architecture as a confidentiality of the user's privacy and security which could result in its wider adoption by masses.

Keywords:

Internet of Things, IoT, IoT security goals, IoT security challenges and issues, IoT security architecture.

1. INTRODUCTION

The term, Internet of Things, a system of interconnected devices, was first proposed by Kevin Ashton in 1999 [1]. It is a major technological revolution that has updated the current Internet infrastructure to a concept of much more advanced computing network where all the physical objects around us will be uniquely identifiable and ubiquitously connected to each other [2]. By this continually emerging technology everything around us like televisions, refrigerators, cars and clothes etc will be collecting some useful data with the help of various existing technologies, which will then be autonomously flowing the data to the concerned devices and on the basis of which automated actions will be taken.

With a number of researches being carried out, the vision of IoT is likely to be a reality very soon. According to Gartner, around 25 billion uniquely identifiable objects are expected to be a part of this global computing network by the year 2020 [3], which is impressively a big number, however prevalence of such a big network of interconnected devices will pose some new security and privacy threats and put all those devices at a high risk of hackers as they clutch at the security gaps to make the devices work for their personal benefits.

IoT definitely has a great potential for flexibility and promises a great future but it has a potential of security disaster too. There are many questions for its wide adoption and without answering them and coming up with proper solutions for the newly posed threats, it does not seem to have any future [4]. Due to easy accessibility of the objects, it can be easily exploited by the evil-minded hackers [5]. No matter how much secure companies think their products are, they are still prone to various kinds of attacks so they must ensure proper security by making the patches available as soon as any vulnerability is detected in the system. Since the devices have a direct impact on the lives of users so security considerations must be a high priority and there must be some proper well-defined security infrastructure with new systems and protocols that can limit the possible threats related to scalability, availability and security of IoT [6].

The paper is organized as follows. Section 2 describes the generic architecture of IoT. Section 3 describes the security goals. Section 4 discusses the major security challenges and issues on each layer. Section 5 presents the security architecture of IoT and finally Section 6 concludes the paper.

2. GENERIC ARCHITECTURE

Generally, IoT has four main key levels as shown in Fig. 1, which are described below [7]:

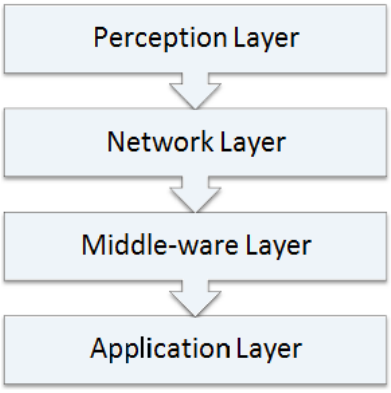

Fig. 1. Generic Architecture of IoT

2.1 Perception Layer

This layer consists of different kinds of data sensors like RFID, Barcodes or any other sensor network [8]. The basic purpose of this layer is to identify the unique objects and deal with its collected data obtained from the real world with the help of its respective sensor(s).

2.2 Network Layer

The purpose of this layer is to transmit the gathered information obtained from the perception layer, to any particular information processing system through existing communication networks like Internet, Mobile Network or any other kind of reliable network [9].

2.3 Middle-ware Layer

This layer consists of information processing systems that take automated actions based on the results of processed data and links the system with the database which provides storage capabilities to the collected data. This layer is service-oriented which ensures same service type between the connected devices [10].

2.4 Application Layer

This layer realizes various practical applications of IoT based on the needs of users and different kinds of industries such as Smart Home, Smart Environment, Smart Transportation and Smart Hospital etc [11].

3. SECURITY GOALS

The major security goals of IoT are to ensure proper identity authentication mechanisms and provide confidentiality about the data etc. The Security triad or CIA triad, a distinguished model for the development of security mechanisms, implements the security by making use of the three areas which are Data confidentiality, integrity and availability as shown in the Fig. 2. A breach in any of these areas could cause serious issues to the system so they must be accounted for. The three areas are described below:

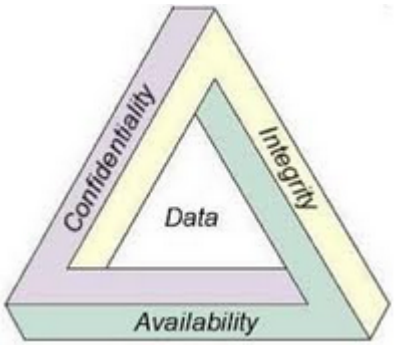

Fig. 2. The CIA Triad

3.1 Data Confidentiality

Data confidentiality is identical to providing freedom to user from the external interference. It is the ability to provide confidence to user about the privacy of the sensitive information by using different mechanisms such that its disclosure to the unauthorized party is prevented and can be accessed by the permitted users only. There are many security mechanisms to provide confidentiality of the data including, but not limited to, Data Encryption in which the data is converted into ciphertext form which makes it difficult to access for the users having no proper authorizations, the Two-step verification, which provides authentication by two dependent components and allows the access only if both the components pass the authentication test and the most common Biometric Verification in which every person is uniquely identifiable. For the IoT based devices, it ensures that the sensor nodes of the sensor networks don't reveal their data to the neighboring nodes, similarly the tags don't transmit their data to an unauthorized reader [12].

3.2 Data Integrity

During the communication, data could be altered by the cybercriminals or could be affected by various other factors that are beyond human control including the crash of server or an electromagnetic disturbance. Data Integrity refers to the protection of useful information from the cybercriminals or the external interference during transmission and reception with some common tracking methods, so that the data cannot be tampered without the system catching the threat [13]. The methods to ensure the accuracy and originality of data includes methods like Checksum and Cyclic Redundancy Check (CRC) which are simple error detector mechanisms for a portion of data. Moreover, continuous syncing of the data for backup purposes and the feature like Version control, which keeps a record of the file changes in a system to restore the file in case of fortuitous deletion of data can also ensure the integrity of data such that the data on IoT based devices is in its original form when accessed by the permitted users.

3.3 Data Availability

One of the major goals of IoT security is to make data available to its users, whenever needed. Data Availability ensures the immediate access of authorized party to their information resources not only in the normal conditions but also in disastrous conditions. Due to dependency of companies on it, it is necessary to provide firewalls to countermeasure the attacks on the services like Denial-of-service (DoS) attack which can deny the availability of data to the user-end. Data Availability also ensure the prevention of bottleneck situations which prevent the flow of information. The Redundancy and Failover backup methods provide duplication of the system components in conditions of system failure or various system conflictions to ensure reliability and availability of data.

4. SECURITY CHALLENGES AND ISSUES

There have been many achievements in the research field of IoT, however there are still some open challenges that needs to be addressed for the ubiquity of this technology. In this section some of the threats in each architectural layer that needs special attention are discussed.

4.1 Perception Layer Challenges

Perception layer consists of different sensor technologies like RFID which are exposed to many kinds of threats which are discussed below:

4.1.1 Unauthorized Access to the Tags. Due to the lack of proper authentication mechanism in a large number of RFID systems, tags can be accessed by someone without authorization. The attacker cannot just read the data but the data can be modified or even deleted as well [14].

4.1.2 Tag Cloning. Since tags are deployed on different objects which are visible and their data can be read and modified with some hacking techniques therefore they can be easily captured by any cybercriminal who can create a replica of the tag and hence compromising it in a way that the reader cannot distinguish between the original and the compromised tag [15].

4.1.3 Eavesdropping. Because of the wireless characteristics of the RFID it becomes very easy for the attacker to sniff out the confidential information like passwords or any other data flowing from tag-to-reader or reader-to-tag which makes it vulnerable because the attacker can make it to use in despicable ways [16].

4.1.4 Spoofing. Spoofing is when an attacker broadcasts fake information to the RFID systems and makes it to assume its originality falsely which makes it appearing from the original source [17]. This way attacker gets full access to the system making it vulnerable.

4.1.5 RF Jamming. RFID tags can also be compromised by kind of a DoS attack in which communication through RF signals is disrupted with an excess of noise signals [18].

4.2 Network Layer Challenges

Network layer consists of the Wireless Sensor Network (WSN) which transmits the data from the sensor to its destination with reliability. The related security issues are discussed below:

4.2.1 Sybil Attack. Sybil is a kind of attack in which the attacker manipulates the node to present multiple identities for a single node due to which a considerable part of the system can be compromised resulting in false information about the redundancy [19].

4.2.2 Sinkhole Attack. It is a kind of attack in which the adversary makes the compromised node look attractive to the nearby nodes due to which all the data flow from any particular node is diverted towards the compromised node resulting in packets drop i.e. all the traffic is silenced while the system is fooled to believe that the data has been received on the other side. Moreover this attack results in more energy consumption which can cause DoS attack [20].

4.2.3 Sleep Deprivation Attack. The sensor nodes in the Wireless Sensor Network are powered with batteries with not so good lifetime so the nodes are bound to follow the sleep routines to extend their lifetime. Sleep Deprivation is the kind of attack which keeps the nodes awake, resulting in more battery consumption and as a result battery lifetime is minimized which causes the nodes to shut down [21].

4.2.4 Denial of Service (DoS) Attack. The kind of attack in which the network is flooded with a useless lot of traffic by an attacker, resulting in a resource exhaustion of the targeted system due to which the network becomes unavailable to the users [22].

4.2.5 Malicious code injection. This is a serious kind of attack in which an attacker compromises a node to inject malicious code into the system which could even result in a complete shutdown of the network or in the worst case, the attacker can get a full control of the network [23].

4.2.6 Man-in-the-Middle Attack. This is a form of Eavesdropping in which target of the attack is the communication channel due to which the unauthorized party can monitor or control all the private communications between the two parties hideously. The unauthorized party can even fake the identity of the victim and communicate normally to gain more information [24].

4.3 Middle-ware Layer Challenges

This layer is composed of data storage technologies like cloud computing. The security challenges of this layer are discussed below:

4.3.1 Unauthorized Access. Middle-ware Layer provides different interfaces for the applications and data storage facilities. The attacker can easily cause damage to the system by forbidding the access to the related services of IoT or by deleting the existing data. So an unauthorized access could be fatal for the system.

4.3.2 DoS Attack. It is similar to the DoS attack discussed in the previous two layers i.e. it shuts down the system which results in unavailability of the services.

4.3.3 Malicious Insider. This kind of attack occurs when someone from the inside tampers the data for personal benefits or the benefits of any 3rd party. The data can be easily extracted and then altered on purpose from the inside.

4.4 Application Layer Challenges

The related security issues of this layer are described below:

4.4.1 Malicious Code Injection. An attacker can leverage the attack on the system from end-user with some hacking techniques that allows the attacker to inject any kind of malicious code into the system to steal some kind of data from the user.

4.4.2 Denial-of-Service (DoS) Attack. DoS attacks nowadays have become sophisticated, it offers a smoke screen to carry out attacks to breach the defensive system and hence data privacy of the user, while deceiving the victim into believing that the actual attack is happening somewhere else. This put the non-encrypted personal details of the user at the hands of the hacker.

4.4.3 Spear-Phishing Attack. It is an email spoofing attack in which victim, a high ranking person, is lured into opening the email through which the adversary gains access to the credentials of that victim and then by a pretense retrieves more sensitive information.

4.4.4 Sniffing Attack. An attacker can force an attack on the system by introducing a sniffer application into the system, which could gain network information resulting in corruption of the system [25].

5. SECURITY AT DIFFERENT LAYERS

There are many researches being carried out to provide a reliable well-defined security architecture which can provide confidentiality of the data security and privacy. W. Zhang et al. [26] proposed an architecture for the security against the possible threats, as shown in Fig. 3.

5.1 Perception Layer

Perception Layer is the bottom layer of the IoT architecture which provides various security features to the hardware. It serves four basic purposes which are Authentication, Data Privacy, Privacy of sensitive information and Risk Assessment which are discussed below:

5.1.1 Authentication. Authentication is done using Cryptographic Hash Algorithms which provides digital signatures to the

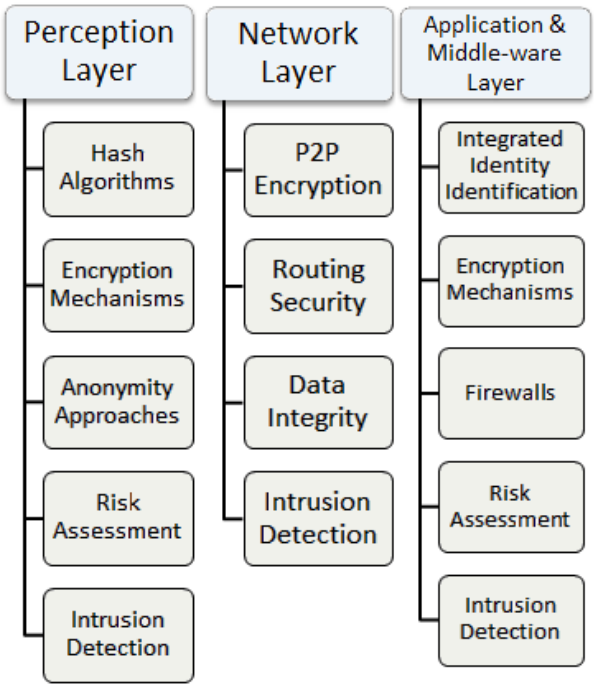

Fig. 3. Security Architecture of IoT

terminals that could withstand all the possible known attacks like Side-channel attack, Brute force attack and Collision attack etc.

5.1.2 Data Privacy. Privacy of the data is guaranteed by symmetric and asymmetric encryption algorithms such as RSA, DSA, BLOWFISH and DES etc which prevents an unauthorized access to the sensor data while being collected or forwarded to the next layer. Due to their low power consumption benefit, they can be easily implemented into the sensors.

5.1.3 Privacy of sensitive information. As for hiding the sensitive information, anonymity of the location and identity is obtained using K-Anonymity approach which ensures the protection of the information like identity and location etc of the user [27].

5.1.4 Risk Assessment. It is a fundamental of IoT security which discovers the new threats to the system. It could help preventing the security breaches and determining the best security strategies. An example of it is the Dynamical Risk Assessment method for IoT [28].

Even with such security measures, if an intrusion is detected in the system, an automated Kill-command from the RFID reader is sent to the RFID tag which prevents an unauthorized access to the RFID tag data [29].

5.2 Network Layer

The network layer which could be both wired or wireless is exposed to various kinds of attacks. Due to the openness of the wireless channels, communications can be monitored easily by some hackers. The network layer security is further divided into three types which are discussed below:

5.2.1 Authentication. With the help of a proper authentication process and point to point encryption, illegal access to the sensor nodes to spread fake information could be prevented [30]. The most common kind of attack is the DoS attack which impacts the network by driving a lot of useless traffic towards it through a number of botnets fueled by the system of interconnected devices.

5.2.2 Routing Security. After the Authentication process, routing algorithms are implemented to ensure the privacy of data exchange between the sensor nodes and the processing systems [31]. There have been many researches carried out for the routing ways including Source Routing [32], in which data to be transmitted is stored in the form of packets which is then sent to the processing system after being analyzed by the intermediate nodes, And the Hop-by-Hop routing in which only address of the data destination is known. The security of routing is ensured by providing multiple paths for the data routing which improves the ability of the system to detect an error and keep performing upon any kind of failure in the system [33].

5.2.3 Data Privacy. The safety control mechanisms monitors the system for any kind of intrusion and finally Data integrity methods are implemented to make sure that the data received on the other end is the same as the original one.

5.3 Middle-ware and Application Layer

This layer amalgamates the Middle-ware and Application layer to form an integrated security mechanism. The security categorization is discussed below:

5.3.1 Authentication. Firstly it goes through the authentication process which prevents the access to any miscreant user by integrated identity identifications. This is exactly similar to that of the identification process in either of the layers except that this layer encourages authentications by some certain cooperating services which means users can even choose the associated information to be shared with the services.
The major technologies used in this layer are Cloud computing and Virtualization, both of which are ripe to various attacks. The cloud technology can be easily compromised, one of the worst threat is the insider threat. Similarly Virtualization is exposed to DOS and data theft etc. A lot of research is needed in both domains to provide secure environment.

5.3.2 Intrusion Detection. Its intrusion detection techniques provide solutions for various security threats by generating an alarm on occurrence of any suspicious activity in the system due to the continuous monitoring and keeping a log of the intruder's activities which could help to trace the intruder. There are different existing intrusion detection techniques [34] including the data mining approach [35] and anomaly detection.

5.3.3 Risk Assessment. The risk assessment gives justification for the effective security strategies and provides improvements in the existing security structure.

5.3.4 Data Security. Data security is ensured by various encryption technologies which prevent the data stealing threats. Moreover, to prevent other malicious activities from the miscreant users, Anti-Dos firewalls and up to date spywares and malwares are introduced.

6. CONCLUSION AND FUTURE WORK

The only hurdle that stands in the way of the IoT development is the security and privacy issues. Security at all the levels of IoT is expository to the functioning of IoT. Luckily, there already have been many research achievements in the IT security concerns and for

effective implementation of a security infrastructure for IoT, these achievements must need to be further expanded instead of focusing the attention towards seeking the new possible security solutions, to make IoT able to provide services to the futuristic data-hungry billions of devices with the ability to thwart the adversaries. So the adequate privacy and security measures through substantial researches must be made and the answers for the number of open questions in this research field must be provided, before it gets deployed in the society. This paper discussed the security goals and possible security challenges and issues of the IoT system. Then a well-defined architecture for the IoT security was presented. In the future, more authentications, risk assessment and intrusion detection techniques in each architectural layer must be explored in parallel to the implementation of the security infrastructure using existing IT security features. Moreover, legal frameworks, proper regulations and policies must be devised to ensure stable development of the secure technologies.

7. REFERENCES

[1] Kevin Ashton, That Internet of things thing, It can be accessed at: *http://www.rfidjournal.com/articles/view?4986*

[2] D. Singh, G. Tripathi, A.J. Jara, A survey of Internet-of Things: Future Vision, Architecture, Challenges and Services, in *Internet of Things (WF-IoT)*, 2014

[3] Gartner, Inc. It can be accessed at: *http://www.gartner.com/newsroom/id/2905717*

[4] Rolf H. Weber, "Internet of Things - New security and privacy challenges," in *Computer Law and Security Review (CLSR)*, 2010, pp. 23-30

[5] Rodrigo Roman, Pablo Najera and Javier Lopez, "Securing the Internet of Things," in *IEEE Computer*, Volume 44, Number 9, 2011, pp. 51-58

[6] Friedemann Mattern and Christian Floerkemeier, "From the Internet of Computers to the Internet of Things," in *Lecture Notes In Computer Science (LNCS)*, Volume 6462, 2010, pp 242-259

[7] Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi Liu, Security in the Internet of Things: A Review, in *Computer Science and Electronics Engineering (ICCSEE)*, 2012, pp. 648-651

[8] Ying Zhang, Technology Framework of the Internet of Things and Its Application, in *Electrical and Control Engineering (ICECE)*, pp. 4109-4112

[9] Xue Yang, Zhihua Li, Zhenmin Geng, Haitao Zhang, A Multilayer Security Model for Internet of Things, in *Communications in Computer and Information Science*, 2012, Volume 312, pp 388-393

[10] Rafiullah Khan, Sarmad Ullah Khan, R. Zaheer, S. Khan, Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges, in *10th International Conference on Frontiers of Information Technology (FIT 2012)*, 2012, pp. 257-260

[11] Shi Yan-rong, Hou Tao, Internet of Things key technologies and architectures research in information processing in *Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE)*, 2013

[12] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini and Imrich Chlamtac, "Internet of Things: Vision, applications and research challenges," in *Ad Hoc Networks*, 2012, pp.1497-1516

[13] Luigi Atzori, Antonio Iera, Giacomo Morabito, "The Internet of Things: A Survey," in *Computer Networks*, pp. 2787-2805

[14] Mr. Ravi Uttarkar and Prof. Raj Kulkarni, "Internet of Things: Architecture and Security," in *International Journal of Computer Application*, Volume 3, Issue 4, 2014

[15] Mike Burmester and Breno de Medeiros, "RFID Security: Attacks, Countermeasures and Challenges."

[16] Benjamin Khoo, "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy," in *IEEE International Conferences on Internet of Things, and Cyber, Physical and Social Computing*, 2011

[17] Aikaterini Mitrokotsa, Melanie R. Rieback and Andrew S. Tanenbaum, "Classification of RFID Attacks."

[18] Lan Li, "Study on Security Architecture in the Internet of Things," in *International Conference on Measurement, Information and Control (MIC)*, 2012

[19] John R. Douceur, "The Sybil Attack," in *Peer-to-Peer Systems - IPTPS*, 2002, pp. 251-260

[20] Nadeem AHmed, Salil S. Kanhere and Sanjay Jha, "The Holes Problem in Wireless Sensor Network: A Survey," in *Mobile Computing and Communications Review*, Volume 1, Number 2

[21] Tapalina Bhattasali, Rituparna Chaki and Sugata Sanyal, "Sleep Deprivation Attack Detection in Wireless Sensor Network," in *International Journal of Computer Applications*, Volume 40, Number 15, 2012

[22] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A survey of ATtacks, Security Mechanisms and Challenges in Wireless Sensor Networks," in *International Journal of Computer Science and Information Security*, Volume 4, Number 1, 2009

[23] Priyanka S. Fulare and Nikita Chavhan, "False Data Detection in Wireless Sensor Network with Secure Communication," in *International Journal of Smart Sensors and AdHoc Networks (IJSSAN)*, Volume-1, Issue-1, 2011

[24] Rabi Prasad Padhy, Manas Ranjan Patra, Suresh Chandra Satapathy, "Cloud Computing: Security Issues and Research Challenges," in *International Journal of Computer Science and Information Technology & Security (IJCSITS).*

[25] Bhupendra Singh Thakur, Sapna Chaudhary, "Content Sniffing Attack Detection in Client and Server Side: A Survey," in *International Journal of Advanced Computer Research*, Volume 3, Number 2, 2013

[26] W. Zhang, B. Qu, Security Architecture of the Internet of Things Oriented to Perceptual Layer, in *International Journal on Computer, Consumer and Control (IJ3C)*, Volume 2, No.2 (2013)

[27] K.E. Emam, F.K. Dankar, Protecting Privacy Using kAnonymity, in *Journal of the American Medical Informatics Association*, Volume 15, Number 5, 2008

[28] C. Liu, Y. Zhang, J. Zeng, L. Peng, R. Chen, Research on Dynamical Security Risk Assessment for the Internet of Things inspired by immunology, in *Eighth International Conference on Natural Computation (ICNC)*, 2012

[29] T. Karygiannis, B. Eydt, G. Barber, L. Bunn, T. Phillips, Guidelines for Securing Radio Frequency Identification (RFID) Systems, in *Recommendations of National Institute of Standards and Technology*

[30] Yassine MALEH and Abdellah Ezzati, "A Review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks," in *International Journal of Wireless & Mobile Networks (IJWMN)*, Volume 5, Number 6, 2013

[31] Z. Xu, Y. Yin, J. Wang, A Density-based Energy-efficient Clustering Algorithm for Wireless Sensor Networks, in *International Journal of Future Generation Communication and Networking*, Volume 6, Number 1, 2013

[32] Shashank Agrawal and Dario Vieira, A survey on Internet of Things.

[33] Chen Qiang, Guang-ri Quan, Bai Yu and Liu Yang, Research on Security Issues of the Internet of Things, in *International Journal of Future Generation Communication and Networking*, Volume 6, Number 6, 2013, pp. 1-10

[34] Animesh Patcha, Jung-Min Park, An overview of anomaly detection techniques: Existing solutions and latest technological trends, in *Computer Networks*, Volume 51, Issue 2, 2007

[35] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic and Marimuthu Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions."