ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 5 May 2017, Page No. 21435-21442
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i5.41

Internet of Things: A Survey on Security Issues Analysis and Countermeasures

B.Sasikala[1], M. Rajanarajana[2], Dr. B. Geethavani[3]
[1]Assistant Professor, Department of Computer Science & Engineering,
GVIC Engineering College, Madanapalli, AP, India.
mrs.sasicse@gmail.com
[2]Assistant Professor, Department of Computer Science & Engineering,
GVIC Engineering College, Madanapalli, AP, India.
mr.ranacse@gmail.com
[3]Professor, Department of Computer Science & Engineering,
Narayana Engineering College, Nellore, A.P, India.
bgeethavani1269@gmail.com

Abstract
The Internet of Things (IoT) is becoming one of the milestones in the era of communication and networking which is going to determine future of IT. The explanation goes on to say that "The Internet of Things is such a radical concept that it is a challenge to even imagine all the possible ways in which it will affect business, economies, and society". Internet-of-Things (IoT) is the junction of Internet with RFID, Sensor and smart objects. IoT can be defined as "things belonging to the Internet" to supply and access all of real-world information. The Internet of Things (IoT) is a pervasive Internet-based network. Although it makes appreciable development, there are still uncertainties about security concepts of its usage that is usually considered as a major concern in the design of IoT architectures. However, the IoT exhibits characteristics that pose considerable risks: inherent openness, heterogeneity, and terminal vulnerability. This paper mainly focusing on survey of analyzing all security issues and suggested countermeasure. And as IoT contains four layers: perception layer, network layer, support layer and application layer, this paper will analyze the security problems of each layer separately. The study defines security requirements and challenges that are common in IoT implementations and discusses security threats and related solutions to make this technology secure and more prevalent accordingly and suggested further areas of research needed.

Keywords: Internet of Things, Layered Architecture, Security Issues, Measures.

1. Introduction

The term, Internet of Things, know as 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 pervasively connected to each other [2] [3]. 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 [7]. There are several fuzziness about the concept of Internet of Things such as IoT can be broken in two parts Internet and Things. The ''things'' are physical objects carrying RFID tags with a unique EPC(Electronic Product Code). Ubiquitous computing which was thought as a difficult task has now become a reality due to advances in the field of Automatic Identification, wireless communications, distributed computation process and fast speed of Internet. Today, Communication is enveloping as there is a growing interest in sharing data through the Internet. With a number of researches being carried out, the vision of IoT is likely to be a reality very soon[5] [7] [8].

According to Gartner, around 25 billion uniquely identifiable objects are expected to be a part of this global computing network by the year 2020 [4], 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. With the rapid development of Internet of Things (IoT), there are a variety of IoT applications, which contribute to our everyday life. They cover from traditional equipment to general household objects, which help make human being's life better. With the development of IoT technology, information insecurity will directly threat the entire IoT system [8] [9].

Nowadays, IoT is widely applied to social life applications such as smart grid, intelligent transportation, smart security, and smart home [15]. Access cards, bus cards and some other small applications also belong to IoT. Applications of IoT can bring convenience to people, but if it cannot ensure the security of personal privacy, private information may be leaked at any time. So the security of IoT cannot be ignored. Once the signal of IoT is stolen or interrupted, it will directly affect the security of the entire information of IoT. With the widely spreading of IoT, it will provide more extensive wealthy of information, the risk of exposure of such information will increase. If IoT cannot have a good solution for security issues, it will largely restrict its development. Thus, above all the problems of IoT, security problem is particularly important. Since the devices are directly connected to the users' day to day life so security considerations must be the highest priority and there must be some proper well-defined security infrastructure to limit the threats related to robustness, availability and security of IoT [6] [8] [9].

This study presents a survey of all the security issues in IoT and countermeasures along with the analysis of IoT architectures. The main objective of this paper is to provide the understanding of security issues of IoT which needs to be studied along with their countermeasures. The paper describes security requirements and challenges that are usually faced in IoT implementations and mentions security issues and related solutions on each layer of IoT architecture to make this technology secure and more prevalent. In the following sections, this paper gives a brief idea of IoT which includes overview of IoT, the architecture of IOT, security issues at each layer, countermeasures and applications.

2. IoT Overview

2.1. What is the Internet of Things?

As shown in Fig. 1, the IoT allow people and things to be connected anytime, anyplace, with anything and anyone, ideally using any path/network and any service [11]. They are "Material objects connected to material objects in the Internet". Definitions for the Internet of Things vary. According to McKinsey: "Sensors and actuators embedded in physical objects are linked through wired and wireless networks, often using the same Internet Protocol (IP) that connects the Internet"[2].

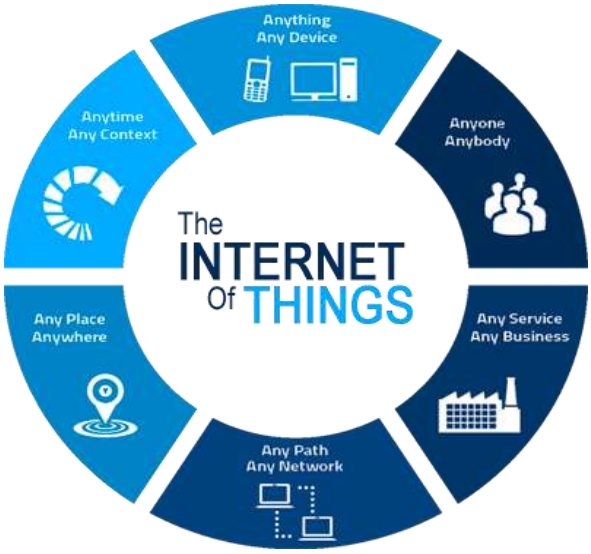

Fig 1: Internet of Things Scenario

2.2 History of IoT

The term Internet of Things is 16 years old. But the actual idea of connected devices had been around longer, at least since the 70s. Back then, the idea was often called "embedded internet" or "pervasive computing". But the actual term "Internet of Things" was coined by Kevin Ashton, cofounder and executive director of the Auto-ID Center at MIT, in a presentation he made to Procter & Gamble in 1999 [1]. Ashton who was working in supply chain optimization, wanted to attract senior management's attention to a new exciting technology called RFID. Because the internet was the hottest new trend in 1999 and because it somehow made sense, he called his presentation "Internet of Things". The concept of IoT started to gain some popularity in the summer of 2010. The same year, the Chinese government announced it would make the Internet of Things a strategic priority in their Five-Year-Plan. In 2011, Gartner, the market research company that invented the famous "hype-cycle for emerging technologies" included a new emerging phenomenon on their list: "The Internet of Things"[4]. The next year the theme of Europe's biggest Internet conference LeWeb was the "Internet of Things". At the same time popular tech focused magazines like Forbes, Fast Company, and Wired starting using IoT as their vocabulary to describe the phenomenon. In October of 2013, IDC published a report stating that the Internet of Things would be a $8.9 trillion market in 2020. The term Internet of Things reached mass market awareness when in January 2014 Google announced to buy Nest for $3.2bn. At the same time the Consumer Electronics Show (CES) in Las Vegas was held under the theme of IoT [2].

2.3 IoT − Key Features

The most important features of IoT include artificial intelligence, connectivity, sensors, active

engagement, and small device use [7]. A brief review of these features is given below:

AI: IoT basically makes virtually anything "smart", meaning it enhances every aspect of life with the power of data collection, artificial intelligence algorithms, and networks. This can mean something as simple as enhancing your refrigerator and cabinets to detect when milk and your favorite cereal run low, and to then place an order with your preferred grocer.

Connectivity: New enabling technologies for networking, and specifically IoT networking, mean networks are no longer exclusively tied to major providers. Networks can exist on a much smaller and cheaper scale while still being practical. IoT creates these small networks between its system devices.

Sensors: IoT loses its distinction without sensors [5] [8]. They act as defining instruments which transform IoT from a standard passive network of devices into an active system capable of real-world integration.

Active Engagement: Much of today's interaction with connected technology happens through passive engagement. IoT introduces a new paradigm for active content, product, or service engagement.

Small Devices: Devices, as predicted, have become smaller, cheaper, and more powerful over time. IoT exploits purpose-built small devices to deliver its precision, scalability, and versatility.

3. Basic Architecture of IoT

IoT architecture is a network formed by interconnected device in any environment for example, home, business or retail to facilitate communication. It consists of four major layers: Perception Layer, Network Layer, Support Layer and Application Layer [10] [13] as shown in the fig: 2.

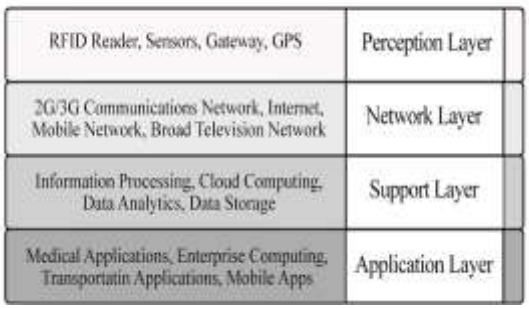

Fig: 2 Architecture of IoT

Perception Layer: This layer consists of different kinds of data sensors like RFID, Barcodes or any other sensor network [6] [8]. The sensor technology, intelligence embedded technology, nano technology and tagging technology are located in this layer. Main purpose of the layer is the identification of distinctive objects and the collection of information from the physical world with the help of its sensors. The main working of IoT i.e. collection of information is done at this layer with the help of different devices like smart card, RFID tag, reader and sensor networks, etc. It has a feature of broad sensing through the RFID system to get object's information anytime and anywhere. Each RFID electronic tag has a unique ID called Electronic Product Code (EPC) which is the only searchable ID allocated for each physical target.

Network Layer: The purpose of this layer is to broadcast 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]. It contains WSN, optical fiber communication networks, broad television networks, 2G/3G communications networks, fixed telephone networks and closed IP data networks for each carrier. Transfer of collected information from sensors, devices, etc., to an information processing system is under the liability of this layer.

Support Layer: This layer consists of information processing systems that take automated events 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]. This layer works very closely with applications. Therefore, researchers prefer to place it in application layer [9] [10].

Application Layer: This layer grasp 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 [9].

4. IoT Security Issues Analysis

Security issues existing in the IoT are closely coupled with its application environment. A detailed discussion is provided as follows.

4.1 Perceptual layer security issues

In the perceptual layer, perceptual nodes usually build an adhoc network with a active distribution. Perception layer mainly includes: Smart card, Reader, RFID tag, Sensor network [8] [9] [14]. Each of these devices has following exposure which leads to be a security issue of IOT

Security issues in the wireless sensor networks (WSNs): WSN includes sensor nodes, actuator nodes and so on. WSN is a collection node hence there is a possibility of security issues. The operations performed in a wireless sensor network can be categorized under three categories: *Attacks on secrecy and authentication, Silent attacks on service integrity, Attacks on network availability.*

Security issues in RFID technology: The RFID tags are open to various attacks from outside due to the incorrect security status of the RFID technology. The four most common types of attacks and security issues of RFID tags are as follows [14]: *Unauthorized tag disabling, Unauthorized tag cloning,* Unauthorized tag tracking and Replay attacks [6] [10] [11] [12] [13] [14].

Physical capture: Many nodes are statically deployed in the area and can easily be captured by attackers and thus, are physically compromised.

Brute force attack: The ability of resource storage as well as the computation of the sensor node are restricted and are most likely to suffer from brute force attack.

Clone node: The hardware structure of several perceptual nodes is simple, and hence, can be easily copied by the attacker.

Impersonation: certification in the distributed environment is very difficult for the perceptual node, allowing for malicious nodes to use a fake identity for wicked or collusion attacks.

Routing attack: Data forwarding and relay exist in the process of perceptual data collection. Thus, intermediate nodes might attack the data during forwarding.

*Denial of service (DoS) attack***:** Nodes can easily be trapped under DoS attack, given their finite processing ability.

*Node privacy leak***:** The attacker can passively or actively steal sensitive information in the node.

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.

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 [6] [8] . This way attacker gets full access to the system making it vulnerable.

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 [12] [14].

4.2 Network layer security issues

The function of the network layer is routing [9]. Network layer consists of the Wireless Sensor Network (WSN) which transmits the data from the sensor to its destination with reliability. The security of the network layer is of two main types: The first is from the security risks of the IoT itself; the second is from the related technologies and protocol defects during design and implementation [8] [9]. In wireless networks, nodes can move freely, they can join or leave the network at any time without any prior certification. This will make wireless networks to be more malicious or vulnerable for the security distress. IoT network should have that capacity to handle such malicious destruction, but as per the researchers existing mechanism is not enough to handle this security issue. The following are attacks taking place in the network layer.

Hello flood attack: Hello flood attack causes high traffic in channels by congesting the channel with a high number of useless messages unusually. Here a single malicious node sends a useless message then that message is replayed by the attacker to create a high traffic.

Homing: In this attack, a search is made in the traffic for cluster heads and key managers which having the capability to shut down the entire network.

Selective forwarding: In this, a compromised node sends few selective nodes instead of all the nodes [8]. The selection of the nodes is based on the requirement of the attacker to achieve his malicious objective and thus such node does not forward packets of data.

Sybil: In this attack, the attacker replicates a single node and then presents it with multiple identities to the other nodes.

Wormhole: Wormhole attack causes relocation of bits of data from its original position. The relocation of data packet is carried out while passing bits of data over a link of low latency.

Acknowledgement flooding: Routing algorithms in sensor-based systems need acknowledgements from time to time. In this type of DoS attack, a malicious node sends false information to destined neighboring nodes by the help of these acknowledgements.

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 [10]. Moreover this attack results in more energy consumption which can cause DoS attack.

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 [13]. 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.

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 [13] [14].

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.

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 [14].

4.3 Middleware layer security issues

The IoT middleware layer mainly provides services for basic tasks such as Web service and application program interface. Hence, the measures taken against Web service attack can also be used for those occurring in the middleware layer. In addition, more attacks may arise as the middleware layer becomes more open. This layer is attacked mainly through

Jamming: This DoS attack occupies the communication channel between the nodes and prevents them from communicating with each other [10]. It exploit the transmission of radio signal to interfere with radio frequencies that used by sensor network. It can be performed either continuously or in an isolated way [8] [11]. In both the cases network will suffer from damage.

DoS attack: The DoS or distributed DoS attack can destroy service availability because Internet attack entails low cost.

Non-permission to access: In an open architecture, if unreasonable access configuration, malicious intrusion, or trapping users with higher permissions into improper operation are present, attackers can easily threaten security by denying permission to access the related service.

Node tampering: Extracting sensitive information is known as node tampering.

Data attacks: Attackers focus on attacks for data service. For example, attackers redo service requests, change data on request headers, and execute parts of data dictionary attacks or middleman attacks.

Session attacks: With a state attached to it, the service access can be viewed as a conversation [13] [14]. Thus, the attacker can hijack or redo sessions to gain illegal access.

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 [8]. The data can be easily extracted and then altered on purpose from the inside.

4.4 Application layer security issues

Application layer mainly includes the bright devices for effective decision making. Each of these has some vulnerability which leads to be an issue of the security of IOT. The attacker is likely to destroy privacy in the application layer by a known vulnerability (e.g., buffer overflow, cross site scripting, and SQL injection), error configuration (e.g., simple password), or improperly obtained higher permission access.

Privacy leak: Given that the application of IoT is executed on common operating systems and hosting services, the attacker can easily steal user data (e.g., user password, historical data, and social relations) by known vulnerabilities [14]. The attacker can also analyze terminal location and identity privacy by the query results, unless the software is promptly updated.

Social engineering: A certain relationship exists among IoT users. However, attackers can easily analyze or obtain additional information that can be used for attacks by social engineering.

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.

Denial of Service 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.

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 pretence retrieves more sensitive information [6] [8] [13] [14].

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.

5. Security Countermeasures

The countermeasures for the security issues of IOT are discussed in this subsection with security objectives.

5.1 Security Objective

Based on the IoT security issues, the need of security is required for IoT system. The major security objective of IoT is to ensure proper identity authentication mechanisms and provide confidentiality about the data etc. The Security triad illustrious a 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. 3. A fall foul of in any of these areas could cause serious issues to the system so they must be accounted for. Therefore looking at the traditional parameters of security demand it needs to build a safe internet system of things, which are as follows,

Data Confidentiality

Data confidentiality is identical to providing freedom to user from the external snooping. It is the ability

to provide confidence to user about the privacy of the sensitive information by using different mechanisms such that its exposé 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 cipher text 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 exclusively 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 unlawful reader [15].

Data Integrity

During the communication, data could be distorted 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 include 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.

Data Availability

One of the major objectives 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 ensures 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

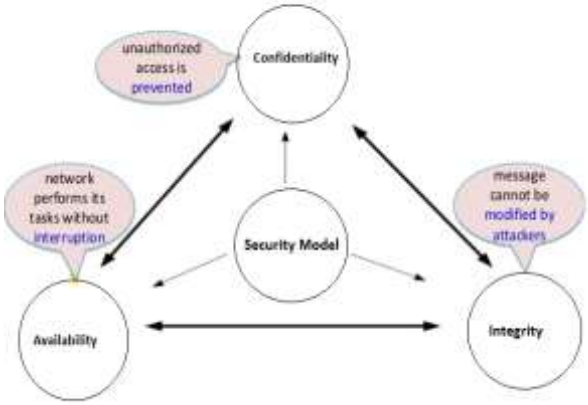

Fig: 3 The Security triad

5.2 IoT Security at Different Layers

The growing use of IOT system needs a powerful protection against all possible attacks or vulnerability. Hence security is needed at each layer of the IOT system. The simple security architecture is shown in fig: 4 Recommended solutions and research directions with respect to security in IoT are examined in three categories: security of perception layer, security of network layer and security of support and application layers.

5.2.1 Security at 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, and Privacy of sensitive information and Risk Assessment which are discussed below:

Authentication: Authentication is done using Cryptographic Hash Algorithms which provides digital signatures to the terminals that could withstand all the possible known attacks like Side channel attack, Brute force attack and Collision attack etc.

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 [11].

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 [6] [8]. 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 [10].

Fig. 4 Security Architecture of IoT

5.2.2 Security at 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:

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 [10] [13]. The commonest of all attacks is DoS attack that influences the network by sending a lot of futile traffic towards it by a number of botnets powered by the system of interconnected devices.

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. There have been many researches carried out for the routing ways including Source Routing, 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 [6] [8] [10] [13]. 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.

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.

5.2.3 Security at 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:

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.

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 [10] [13] including the data mining approach and anomaly detection.

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

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. Applications of IoT

The potentialities offered by the IoT make it possible to develop numerous applications based on it. All the applications are comprised in many more smart "things" such as sensors, actuators, microcontrollers etc. Antoine de Saint-Exupery [16] classifies IoT applications are three major categories they are Society, Environment, Industry. Based on the classification the term "Things" can be professed in a different way and depending on the application domain in which it is used.

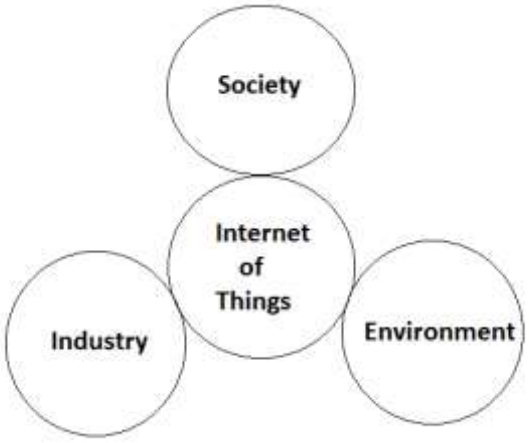

Fig. 5 Classification of IoT Applications

In Industry all IoT Activities are involving in financial or in commercial transactions among companies, organizations and other entities such that Manufacturing, logistics, Service Sector, Banking, Financial Governmental Authorities, Intermediaries, etc. On the whole the "Thing" may typically be the product itself, the equipment, transportation means, etc; everything that participates in the product lifecycle

In Environment applications based on the activities regarding the protection, monitoring and development of all natural resources such as Agriculture & breeding, recycling, environmental management services, energy management, etc.

In Society the whole "Thing" may be related to devices within public spaces or devices for Ambient Assisted Living, etc. For example Agriculture & breeding,

recycling, environmental management services, energy management, smart home, smart city, smart office etc.

7. Conclusion

IoT is a move towards a big achievement in communication network. It should be considered as a part of future internet as everything is going to be connected in a network so that objects can interact with each other, but still there are lots of issues which are to be solved to make this a reality. IoT cannot be used if it is not safe. In future research on the IoT's will remain a hot topic as it is an upcoming technology of innovation but still at its early stages of research and development. In this survey we summarized an overview of IoT including its architecture, history of IoT and some key features. After that we discussed security issues of IoT, some countermeasures and applications.

Reference

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

[2] Knud Lasse Lueth, " IOT basics: Getting Started with Internet of Things".

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

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

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

[6] 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).

[7] Shashank Agrawal and Dario Vieira, A survey on Internet ofThings.

[8] Aaditya Jain, Bhuwnesh Sharma, Pawan Gupta, "INTERNET OF THINGS: ARCHITECTURE, SECURITY GOALS, AND CHALLENGES- A SURVEY" in International Journal of Innovative Research in Science and Engineering, Vol. No. 2, Issue 04, April 2016.

[9] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges", Wireless Networks, 2014, vol. 20, no. 8, pp. 2481–2501.

[10] Engin Leloglu, "A Review of Security Concerns in Internet of Things" Journal of Computer and Communications.

[11] J. Sathish Kumar, Dhiren R. Patel," A Survey on Internet of Things: Security and Privacy Issues", International Journal of Computer Applications (0975 – 8887) Volume 90 – No 11, March 2014.

[12] Mayuri A. Bhabad, Sudhir T. Bagade, "Internet of Things: Architecture, Security Issues and Countermeasures" International Journal of Computer Applications (0975 – 8887) Volume 125 – No.14, September 2015.

[13] Eeshan Pandey, Varshi Gupta, "An analysis of Security Issues of Internet of Things (IoT)" in International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 11, November 2015.

[14] Suchitra.C, Vandana C.P, "Internet of Things and Security Issues", IJCSMC, Vol. 5, Issue. 1, January 2016, pg.133 – 139

[15] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, "*Internet of Things (IoT): A vision, architectural elements, and future directions*", Elsavier - Future Generation Computer Systems, Vol.29, pp. 1645–1660, 2013.

[16] White Paper: "*Internet of Things Strategic Research Roadmap*",
Antoine de Saint-Exupery, 15 sep 2009.

Author Profile

B.Sasikala has received the B.Tech degree in Computer Science and Engineering from JNTUA University in 2009 and M.Tech degree in Computer Science and Engineering from JNTUA University in 2012. She is working as a Assistant Professor in Department of Computer Science & Engineering at GVIC Engineering College, ,Madanapalli, AP, India.

M. Rajanarayana has received the B.Sc Computer Science form SV University in 2000, M.Sc in Compurt Science form Sk University in 2002 and M.Tech in Computer Science and Engineering from JNTUA University in 2012. He is working as a Assistant Professor in Department of Computer Science & Engineering at GVIC Engineering College, ,Madanapalli, AP, India.

Dr. B. GeethaVani has received the B.Tech degree in Computer Science and Engineering from JNTU Hyderabad in 1993 and M.Tech degree in Computer Science and Engineering from JNTU Hyderabad in 2002. She has obtained Ph.D in Computer Science and Engineering from JNTU Kakinada in 2015.She is working as Professor in Computer Science and Engineering Department at Narayana Engineering College, Nellore, A.P. Her research interests include Theory of Computation, Artificial Neural Networks, Image Processing and Information Security.