International Innovative Research Journal of Engineering and Technology

ISSN NO: 2456-1983

International Conference on Emerging Innovation in Engineering and Technology

ICEIET-2017

A Survey Overview of Internet of Things: Applications and Security

V. Parthasaradi[1], P. Kailasapathi [2]

[1] Research Scholar, [2]Professor & Head
Department of Electronics and Communication Engineering, Annamalai University
[1]Saradi.66@gmail.com,[2]Kailasapathy1958@gmail.com

Abstract— Internet of Thing (IOT) appears to be the emerging wafer edge for enabling easy way of connectivity to automate manual routines and reduce human interference. The paper introduces the technology with a security perspective and throws light on the key challenges associated with its outreach. It engages a review of the related issues and opens up the research paths that can form the future work in assuaging the IOT encounters to the utility world. The fact that it shares information on the Internet makes it vulnerable to attacks and data thefts and augurs measures to ensure its safe compliance. The ubiquitous nature of the framework urges to differentiate between malicious or malfunctioning data and explore fresh application to its usage in wearable devices, home and industry appliances.

Keywords—Internet of Things, Application, Security, Challenge

I. INTRODUCTION

The IOT is a objects or "things" of a sensors, Network connectivity and embedded computing systems that can be organized with any other network enabled machine or objects, is of increasing interest for education system. The Internet of Things representations the hidden data and communication layer of the Internet to expose the imperceptible world around us as data for determination and use. With the fast growth of Internet knowledge and communications knowledge, in daily life are regularly led into an imaginary space of virtual world. People can shop, work, chat, keeps pets and plants in the virtual world provided by the network. Based on a large number of wireless communication and low-cost sensors, the sensor network knowledge puts forward new commands to the Internet technology. It will bring massive changes to the future people; change the business models and way of life. Apart from gains of Internet of Things, there are lots of privacy and security concerns at different layers via; Network, Back end and Front end. Internet of Things is an application field that integrates different social field and technological these are outline in Figure1.Despite the diversity of research on IOT, its definition remains fuzzy.

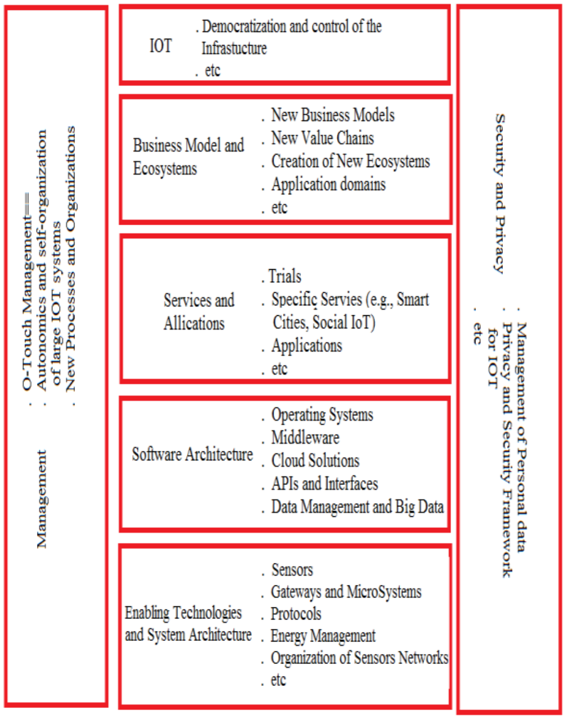

Figure.1 Technological Social Aspects Related To IOT

Definition that addresses all the IOT aspects can facilitate a lead to further research, better understanding of the subject, and advance for us to understanding of this emerging concept.

II. GENERIC ARCHITECTURE:

The organization of IOT encapsulates the five major layers as seen from Figure. 2 and forges to execute the different operations in its functionality.

1. Perception Layer: The sensor devices in the layer include the Infrared sensor, 2D-barcode or RFID depending upon the identification method along with the physical objects. It deals with the identification and collection of specific information by the sensor devices.

2. Network Layer: called as the 'Transmission Layer' transfers the information from the sensor devices to the information processing system. The transmission medium can be wired, wireless, ZigBee, infrared, Bluetooth, Wi-Fi, UMTS and 3G among others depending upon the sensor devices.

3. Middleware Layer: The devices over the IOT device connect and communicate with only those other devices which implement the same type of service. It receives the information from the network layer and performs information processing, ubiquitous computation and takes automatic decision based on the results. The layer with a strong link to the database scores the responsibility for operating the service management facility.

4. Application Layer: It offers to manage the application based on the objects information processed in the Middleware layer. The range of applications spread across smart health, smart farming, smart home, smart city and intelligent transportation.

5. Business Layer: The real success of the IOT technology depends on the business models and augurs to develop them based on the data received from Application layer.

It holds responsibility for the management of overall IOT system including the applications and services and orients to determine the future actions and business strategies

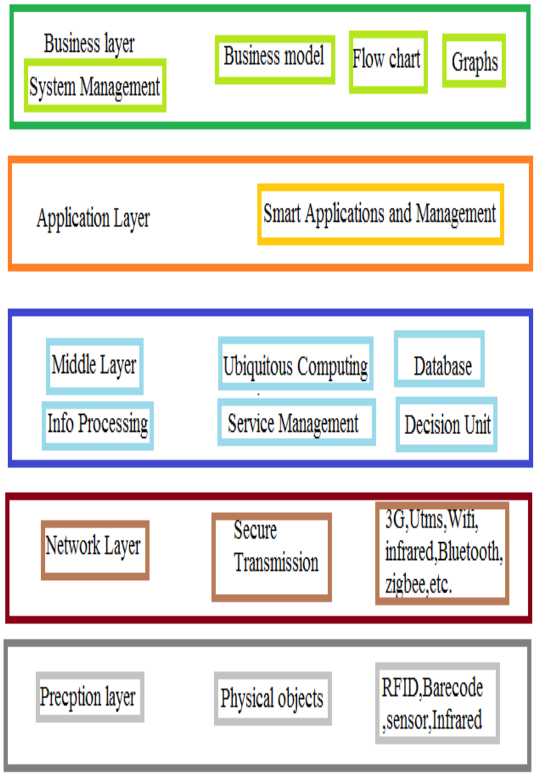

Figure 2.The IOT Architecture

.

III. Features and Definition of Internet of Things:

The IOT be-hives a set of features that a system requires and defines them in accordance with the subject of interest in a perspective to create a clear picture for the user. The features include the following. **Interconnection of Things:** It revolves around the interconnection of "Things" and refers to any physical object that engages to be significant from a user or application perspective.

Connection of Things to the Internet: The "Things" remain connected to the Internet and accordingly deduces to be either an Intranet or Extranet of Things.

Uniquely Identifiable Things: It comprises of things that gather to be uniquely identifiable.

Ubiquity: It echoes to be a major feature of an IOT system, which allows the network to be available anywhere and anytime according to the ITU's definition ITU, SERIES Y, 2005). However the concept "anywhere" and "anytime" may not refer to the ideas of "global" and "always." The terms "anywhere" and "anytime" relates to the concept of where it becomes necessary.

Sensing/Actuation capability: The sensors/actuators acquire a connection to the "Things" and perform the sensing/actuation which bring the smartness of the "Things."

Embedded intelligence: functions as tools for smart and dynamic objects with emergent behavior and become an (external) extension to the human body and mind.

Interoperable Communication Capability: The IOT system inherits a communication capability based on the standard and interoperable communication protocols.

Self configurability: The heterogeneity of devices that include sensors, actuators, storage devices, utility monitoring devices, mobile phones, network elements and computers along with the sheer number of devices that remain connected to the Internet under the IOT umbrella exhibit the fact that the remote or cloud based control appears to be a daunting task and as a consequence suffers from limited scalability. Hence there arises a natural direction for IOT devices to manage themselves both in terms of their software/hardware configuration and their resource utilization.

Programmability: The "Things" of an IOT system at the simplest level reflects a programmable device that can take on a variety of behaviors at a user's command without requiring physical changes.

IV. Applications of the Internet of Things

The IOT can find its applications in almost every aspect of our daily life. Below are some of the examples.

Prediction of natural disasters: The combination of sensors and their autonomous coordination and simulation will help to predict the occurrence of land-slides or other natural disasters and to take appropriate actions in advance.2) **Industry applications:** The IOT can find applications in industry e.g., managing a fleet of cars for an organization. The IOT helps to monitor their environmental performance and process the data to determine and pick the one that need maintenance3) **Design of smart homes**: The IOT can help in the design of smart homes e.g., energy consumption management, interaction with appliances, detecting emergencies, home safety and finding things easily, home security etc.4) **Medical applications:** The IOT can also find applications in medical sector for saving lives or improving the quality of life 5) **Agriculture application:** A network of different sensors can sense data, perform data processing and inform the farmer through communication infrastructure e.g., mobile phone text message about the portion of land that need particular attention. This may include smart packaging of seeds, fertilizer and pest control mechanisms that respond to specific local conditions and indicate actions. Intelligent farming system will help agronomists to have better understanding of the plant growth models and to have efficient farming practices by having the knowledge of land conditions and climate variability. This will significantly increase the agricultural productivity by avoiding the inappropriate farming conditions.6) **Design of smart cities:** The IOT can help to design smart cities e.g., monitoring air quality, discoverin emergency routes, efficient lighting up of the city, watering gardens etc.7) **Smart metering and monitoring:** The IOT design for smart metering and monitoring will help to get accurate automated meter reading and issuance of invoice to the customers. The IOT can also be used to design such scheme for wind turbine maintenance and remote monitoring, gas, water as well as environmental metering and monitoring.

V. SECURITY AND CHALLENGES:

The IOT reference model gives an architectural overview of all the layers involved in a complete full functional IOT system is shown in figure 3. Security of data transmitted is a key challenge, due to integration of more than one technology to make the system functional. This section will give some clarity on the security that is implemented in different layers in the current industry.

Physical Devices & Controllers:

The physical devices and controllers are the "Things" of IOT. This layer consists of device, end nodes, sensors of all types. The security involved in this layer can be a wired or wirelesshandshaket. hrough either of RS232, SPI or RF protocol. This is predominantly to validate the data from a functional or range standpoint. At this layer, data is not validated based on source to detect vulnerability and authentication issues.

Connectivity:

This layer accommodates technologies that help these IOT systems communicate within themselves and with others. These technologies are called Enabling Technologies. Some of the most common enabling technologies are Wired and wireless protocols. Wired protocols such as CAN, J1939, USB, SPI, RS232 and so on. Wireless technologies include but not limited to ZigBee, Bluetooth, Wi-Fi, RF, Cellular and others.

Security in Wired Communication:

Wired communications include but not limited to CAN, J1939, RS232, SPI. Usually RS232 and SPI are within the device or system and it’s peer to peer. Hence the need for security in these types of devices is very less. But protocols like CAN, J1939, USB involve more than one device. Hence the need for security is more in order to fight vulnerability issues. Every device comes with a manufacturer defined hard coded number called the serial number or part number. When it creates the network as a master, or when it joins the network as a device, it gets a network based address. A combination of the serial/part number and the network address is used as a key, for s secured communication in these networks.

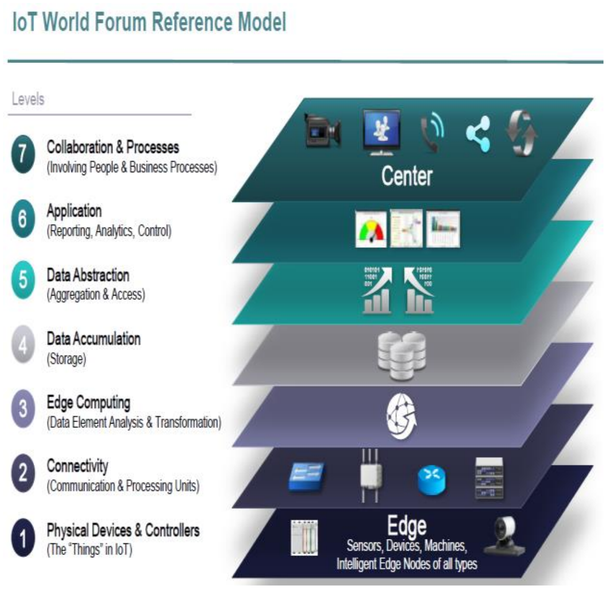
IoT World Forum Reference Model
Levels
7 Collaboration & Processes (Involving People & Business Processes)
6 Application (Reporting, Analytics, Control)
5 Data Abstraction (Aggregation & Access)
4 Data Accumulation (Storage)
3 Edge Computing (Data Element Analysis & Transformation)
2 Connectivity (Communication & Processing Units)
1 Physical Devices & Controllers (The "Things" in IoT)
Center
Edge
Sensors, Devices, Machines, Intelligent Edge Nodes of all types

Figure.3 IOT Architectural overview

Some wired protocols allow secured communication, while some do not. In networks, which allow secured communication, every data is secured (encrypted at source and decrypted at destination). In networks which does not allow secured communication like CAN/J1939, but still if security is needed, manufactures or application developer follow a strategy of defining the security and securing the devices at start-up. They also poll for the device and its info, at a periodic interval, to refresh the secured devices connectivity status.

Security in Wireless communications:

Bluetooth also defines its own security algorithms, as per Bluetooth consortium. Bluetooth controls the security of devices by a pairing mechanism, which is most commonly used in all mobile phones, Car audio system and high data rate audio/video systems. Since Bluetooth is a peer-to-peer communication, security is involved only during connection establishment. ZigBee deploys its proprietary 128-bit AES algorithm for secured communication within its network. User or application can choose to send the data with or without security based on the sensitivity of the data. The difference between the secured and unsecured data transmission is the payload length. Secured data transmission can carry fewer payloads of data than the unsecured one. Since zigbee is a multi hop network, data also traverses multi hop with appropriate security defined by ZigBee.org.

Security in RF is user defined. Since there is no definite standard established, users define their own standards. Advantage of such implementations is that, they provide high data security. However, the interoperability is a big issue, since more than one proprietary mechanism cannot handshake with each other unless both are standardized.

Edge Computing & Data Storage:

Edge Computing supports a wide range of technologies from wireless sensor networks to mobile data acquisition, peer-to-peer ad hoc networking and processing, local cloud computing and grid/mesh computing, distributed data storage and retrieval, and more. Storage as a business and as a need for common man, is gaining more importance than ever before. And due to the current stage of devices like the mobile and the auxiliary devices connected through mobiles and related apps like Point-of-Sales (PoS), retailoutlets, sales and distribution, the volume of data collected through these edge devices increases manifold day-by-day. These data requires mass storages to be stored and retrieved as quick as possible and as needed. Hence the security of data storages which is mostly hard disk (centralized and distributed) and cloud is becoming a challenge. Internet service providers, who initially had only user id and password, are now gong the next step with one time dynamic password and also integrating other forms of security such as bio metrics and iris recognition.

Data Abstraction & Applications:

Data abstraction in IOT is a huge industry on its own. The security perspective in this stage is huge as this is more prone to vulnerability and authentication issues. The data in IOT is very dynamic and real time. Since the data and applications are all exposed through apps, the identification of malfunctioning data and malicious data is a key in IOT security..

Malicious data are those which are actually by unintended players to cause damage to the network in any capacity. Since the data is mostly real-time and the applications are also distributed, Artificial intelligence and machine learning are gaining importance in IOT industry. Hence the need to implement accurate algorithms and security mechanism is increasing.

VI. CHALLENGES:

Following are some of the issues and challenges related to security for IOT.

1. Security can be resource consuming. When using low power embedded device, this can be a even big challenge. The computation power available in IOT is limited and may be insufficient for the processing of security algorithms. The battery capacity is also limited and their life duration is strongly connected to the quantity of computation executed in embedded processor.
2. Cryptography is notoriously expensive and it makes security impossible for resource constrained devices.
3. The complexity and size of some protocols and algorithms makes security expensive.
4. The environment in which those devices are placed can be accessed more easily than fix systems by attackers. Indeed they must be secure against both logical and physical access by malicious entities

VII. CONCLUSION

This paper introduced the emerging future form of Internet called "Internet of Things" that will connect everything and everyone. Security is one of the many parameters that may affect the deployment of IOT. In this paper, a brief introduction to the technology it itself and its security has been explained, Coupled with key enabling technologies that are involved. This survey also points out a probable research direction that could be the future work for the solutions to the security challenges and issue that IOT encounters.

REFERENCE

1. Dmitry Zegzhda ,Tatiana StepanovaAchieving Internet of Things Security via Providing Topological Sustainability Science and Information Conference July 28-30, 2015.
2. Vasileios Karagiannis1, Periklis Chatzimisios1, Francisco Vazquez-Gallego2, Jesus Alonso-Zarate2" A Survey on Application Layer Protocols for the Internet of Things Transaction on IOT and Cloud Computing 2015.
3. Surapon Kraijak, Panwit Tuwanut "A Survey On Internet Of Things Architecture, Protocols, Possible Applications, Security, Priva Cy, Real-World Implementation And Future Trends" Proceedings of ICCT20 15 978-1-4673-7005-9 115/$31.00 ©2015 IEEE.
4. Kim Thuat Nguyen a,⇑, Maryline Laurent b,1, Nouha Oualha a, "Survey on secure communication protocols for the Internet of Things" Elsevier B.V. All rights reserved1570-8705/_ 2015.
5. Jeschke, "The Internet of Things in Production Technology:Heterogeneous Agent Systems for Decentralized ProductionParadigms",6 Expertenforum "Agenten im Umfeld von Industrie 4.0", 2014
6. 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.
7. J. S. Kumar, D. R. Patel. A Survey on Internet of Things: Security and Privacy Issues. International Journal of Computer Applications. 2014.
8. Tasos Kaukalias and Periklis Chatzimisios, Internet of Things (IOT) C Enabling technologies, applications and open issues, Encyclopedia of Information Science and Technology(3rd Ed.), IGI Global Press, 2014.
9. C. Qiang, G. Quan, B. Yu, L. Yang, "Research on Security Issues of the Internet of Thigs", Internatiional journal of Future Generation Communication and Networking, vol. 6, no. 6 (2013).
10. Isam Ishaq *, David Carels, Girum K. Teklemariam, Jeroen Hoebeke, Floris Van den Abeele, Eli De Poorter, Ingrid Moerman and Piet Demeester" IETF Standardization in the Field of the Internet of Things (IOT): A Survey, J. Sens. Actuator Netw. 2013, 2, 235-287; doi:10.3390/jsan2020235.
11. R. Hummen, H. Wirtz, et al., Tailoring end-to-end IP security 1193 protocols to the Internet of things, in: 21th International 1194 Conference on Network Protocols (ICNP), 2013.
12. Li, Lan. "Study on Security Architecture in the Internet of Things." In 2012 International Conference on Measurement, Information and Control (MIC), 1:374–77, 2012. doi:10.1109/MIC.2012.6273274.
13. < www.ijcaonline.org>.
14. < en.wikipedia.org>.
15. < internetofthingswiki.com>.