

A Survey on Internet of Things : Applications and Layered Wise Security Issues

Uppuluri Sirisha¹, Dr. G. Lakshme Eswari²

¹Assistant Professor, Part Time Gitam's Scholar, Department of CSE, Narsimha Reddy Engineering

College, Hyderabad, Telangana, India

²Associate Professor, Department of CSE, GITAM University, Vishakhapatnam, Andhra Pradesh, India

ABSTRACT

This paper briefly introduces Internet of Things(IOT) as a intellectual connectivity among the physical objects or devices which are gaining massive increase in the fields like efficiency, quality of life and business growth. IOT is a global network which is interconnecting around 46 million smart meters in U.S. alone with 1.1 billion data points per day[1]. The total installation base of IOT connecting devices would increase to 75.44 billion globally by 2025 with a increase in growth in business, productivity, government efficiency, lifestyle, etc., This paper familiarizes the serious concern such as effective security and privacy to ensure exact and accurate confidentiality, integrity, authentication access control among the devices.

Keywords : Internet of Things, Threats, Layered Security, Privacy

I. INTRODUCTION

The need of Internet is rapidly increasing in millions of human life's because of the huge development in technological applications in IOT. Now a days people not only using Internet for entertainment purpose but also to fulfill their daily tasks and needs that can't be done without internet. According to a joint report by IAMAI (The Internet and Mobile association of India) & Deloitte the number of IOT devices in India is around 60 million and the number is going to increase to 1.9 billion by 2020. It is estimated that global IOT market would reach \$318 billion by 2023. With an increase level in the growth of IOT technological applications & devices, security and Privacy concerns are also booming into the lime light. In this paper, we are going to discuss about applications, security and privacy concerns related to IOT through a layered architecture.

II. METHODS AND MATERIAL

2. IOT Overview & Background

2.1 What is Internet of Things?

Internet of things is a ubiquitous technology which ensures smart human being's life by connecting physical objects through the network line with the help of internet. The "thing" in Internet of Things refer to in-built sensors which help for communication between the objects through IP addresses. Generally they have the ability to collect and transfer the information over the network line. This sensors use various types of connections such as RFID(radio frequency identification), Wi-Fi, Bluetooth & Zigbee along with wide area connectivity technologies like GSM, GPRS, 3G & LTE. For, example an IOT technology consists of extraordinary number of objects of all shapes and size like a microwave (which cooks your food

automatically in right length of time), self-driving cars (with the help of in-built sensors it generates its path automatically), wearable fitness devices (which counts the number of steps, heart rate, calories burn) etc.,

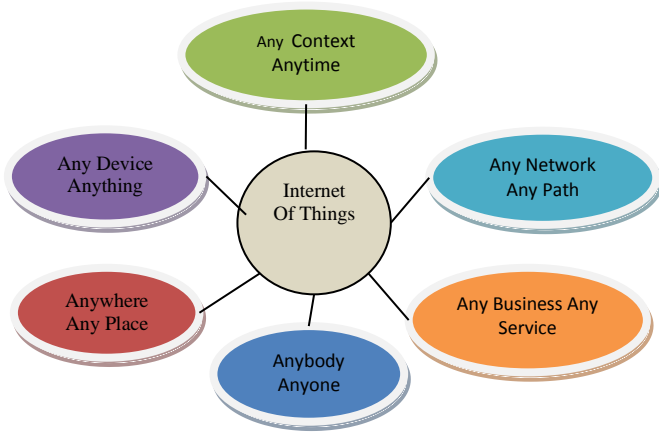




Fig.1 Definition of Internet of Things








2.2 IOT past and present : The History of IOT, and where it's Headed

Invention of Internet of Things:

The actual idea of connected devices was often called “embedded internet” or “pervasive computing” in 70’s. The actual tem “internet of Things” was coined by Kevin Ashton in 1999[2] during his work as a co-founder of MIT’s Auto-ID centre.

Evolving Concepts

Sno	Year	Remarks
1	1992	 with the help of the emergence of Ethernet and Transmission Control Protocol/ Internet protocol (TCP/IP) companies proposed solutions like Microsoft’s at work or Novell’s NEST.
2	1999	 The Internet of Things was coined by Kevin Ashton which helps the legacy devices to connect to internet, extending connectivity to industrial things

3	2009	 After the development of refrigerator, Bluetooth enabled devices, printers, laptops & PC’s the term Internet of Things (IOT) became more popular. By 2009 devices connected to the internet exceeded the number of people.
4	2012	 By this time Cisco, IBM, Ericsson started developing large scale educational & marketing initiatives on IOT. Tracking of the home appliances was one of the first application of IOT.
5	2013	 Building of Internet of Things with IPv4,IPv6 and other hardware platforms were taken place which made the availability of IOT devices accessible in large count.
6	2014	 By 2014, almost 65 percent of respondents has deployed their IOT technologies in the enterprise by turning the society to a smart hub society.
7	2015	 A brief overview of the IOT system design is presented with some typical issues that have to be seen during deployment phase.
8	2016	 Smart living environments, smart farming, food security, wearable’s, ecosystems, autonomous vehicles’ were the major multiple applications programs evolved using IOT technology.
9	2017	 IOT is one of the transformational trends that will shape the future of business in 2017 and beyond.




10	2018	 Roughly around 7 billion IOT devices were connected via WLAN & WPAN by the end of 2018
11	2019	 The major trends that can be expected in 2019 are expansion of applications regarding health care & manufacturing industry, 5G network, edge computing, providing security with less stress.
12	2020	 The predictions regarding IOT's growth perspective are discrete manufacturing , connected industry, smart cities, artificial intelligence, routers with more security, employment opportunities.

Table 1. Evaluation concepts of IOT

2.3 Building the IOT

At the start of IOT emergence, manufacturers shown little interest in IOT technology. So, IOT devices based on RFID(Radio Frequency Identification) technology production stock was less. In June 2000 [1], the world's first inter-connected refrigerator by LG Internet Digital DIOS had appeared with the availability of network connection with WAN port (This idea came into existence in 1997 even before the term Internet of Things was introduced by Kevin Ashton in 1999). The expansion of IOT had increased immensely by implementing more real world applications in 21st century. In 2008,IPSO Alliance is an non-profit organization had formed a collaboration of industry partners with members from technology, communications, energy companies to promote the Internet Protocol (IP) for smart objects[3].

Importance of IOT:

The growth of Internet of Things is increased immensely to a massive scale in the recent years . Internet of Things is no longer just about a high end inter connected appliances but now a days it's common for all types of devices, from TV's to thermostats for cars. The several key factors which are responsible for the growth of IOT are expansion of networking capabilities, introduction to large-scale data analytics tools, creation of new standards such as All Seen Alliances AllJoyn(Open Source standard which makes it easier for IOT hardware and software to interact with different vendors). IOT has evolved by generating huge amount of data from the connected devices, Cloud computing came as a solution for the problems arisen from data storing and communication between the inexpensive sensors [5]. Public Cloud services offered for IOT can easily help the IOT devices to communicate by providing third party access to the infrastructure with greater scalability, performance, pay-as-you-use concept.

3. Architecture of IOTs with common Security Threats and IOT Protocol Stack

3.1 Three Layered Architecture

The following architecture gives basic idea about three layered IOT architecture. Perception layer, Network layer, Application layer are the three layers which are participating in the three layered architecture as shown in Figure 2.

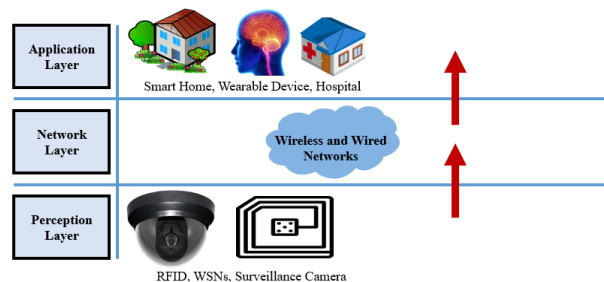


Fig.2 : The three-layered architecture of IoT

3.1.1 Perception Layer

Perception layer is responsible to identify the things and collect information from them with the help of sensors that are attached to the objects. There are various types of sensors like RFID, 2-D barcode, Temperature, gas, Water quality, etc., which are on basis of application we are using. As the basic information like about the location, changes in the environment, changes in motion of a human body can be collected with the help of these sensors, attackers can easily target these sensors and utilize their data for their own by replacing the sensors. So, there is a high chance of getting threats from perception layer.

Common security threats of perception layer:

- **Eavesdropping:** It is an unauthorized real time attack where users private information like phone calls, text messages, fax transmission, video conferences are intercepted by an attacker over a unsecure transmission.
- **Node Capture:** In this attack the key node is attacked by the attacker by gaining full control over the node. As the key node is attacked all the information is leaked including the communication between the sender and receiver.
- **Fake nodes and Malicious:** The energy from real nodes is consumed by the fake nodes which are created by the attacker who aims to stop transmission of information between the sender and the receiver.
- **Replay Attack:** In this attack the intruder through eavesdropping takes the authentication information from sender and send a request to the receiver with fake identity and authentication ID.
- **Timing Attack:** In this attack the intruder just discovers the vulnerabilities in the device computing environment.

3.1.2 Network Layer

Network layer acts a bridge between perception layer and application layer as it transmits the information that has been collected from the physical objects through sensors. Here the medium of transmission can either be wired or wireless which connects smart things, network devices, networks to each other. The prominent that are to be concerned in this layer are about security and authentication.

Common problems and security threats to network layer:

- **Denial of Service (DoS) Attack:** “Denial of service” the term itself describes that this attack prevents the authenticated user from accessing the devices by flooding the network resources with redundant requests.
- **Man-in-The-Middle (MiTM) Attack:** As MiTM attack manipulates the real time data communication between the sender and receiver it is becoming a serious threat to online security.
- **Storage Attack:** Storage device or cloud are used to store the user’s information, which can be attacked by the attacker by modifying the users data with fake details.
- **Exploit Attack:** It generally aims for the internal security vulnerabilities in the application, system software or hardware to get control over the system and to steal store information on a network.

3.1.3 Application Layer

Application layer is responsible for providing services to the applications depending upon the information collected from the sensors. Some of the example applications of IOT are smart homes, smart cities, animal tracking, smart health, etc.,. Security is one of the key concern in application layer, for example if we consider for smart homes the usage of low storage devices such as ZigBee and weak computational

power devices are becoming the key issues to implement strong security.

Common problems and security threats of application layer:

- **Cross Site Scripting:** It is also known injection attack as the attacker injects an unwanted script (like java script) into the client side website to change the contents of the original application to his own needs in an illegal way.
- **Malicious code Attack:** The undesired effects caused by unwanted code in the software is responsible for the malicious attack which cannot be controlled or blocked by any anti-virus.
- **The ability of dealing with mass data:** Network disturbances and data loss are occurred because of huge data collection and transmission between the physical objects through sensors.

3.2 Four Layered Architecture

A four layered architecture is proposed to overcome inefficiencies arisen in the three layered architecture by the researchers. The four layers: Perception layer, Network layer, Support layer, Application layer are illustrated in figure 3.

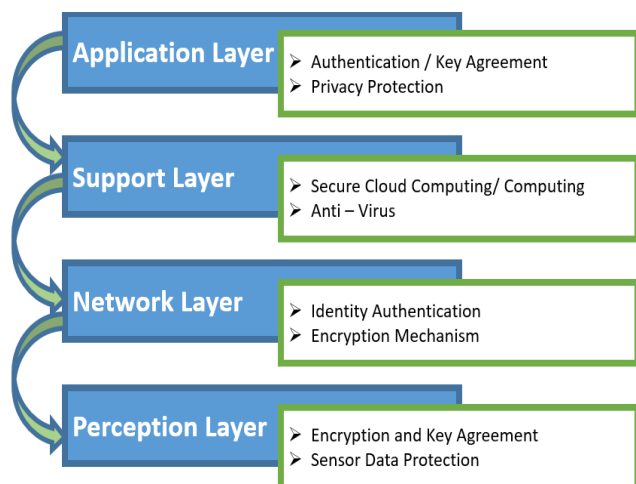


Fig 3. Four layered Architecture of IOT

3.2.1 Support Layer

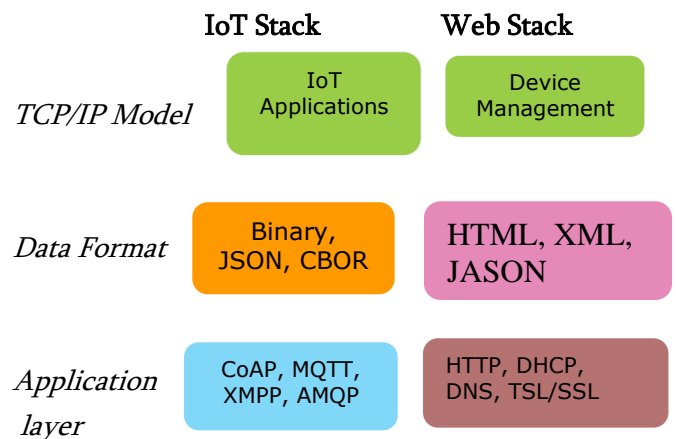
As the information is directly passed from network layer to application layer an additional layer called support layer has been introduced to gain security. The responsibility of support layer is: authentication, protection by using pre-shared secrets, keys and passwords and information passing between network layer and support layer either by wired or wireless medium.

Common problems and security threats of the support layer:

- **DoS Attack:** In this attack the attacker sends unrelated information in bulk by increasing the network traffic between the sender and the user. The IOT gets exhausted by the massive consumption of the resources making the user unable to access the system.
- **Malicious Insider Attack:** It is a complex attack because the attacker is an authorized user who attacks the other users in the network by making it as a attack happened from IOT environment. So, it requires different mechanisms to prevent such attacks.

3.3. Top Protocols used in IOT

The figure 4 shows the IOT protocols that have been standardized for each layer of TCP/IP model including Network, Internet, Transport and Application Layers.



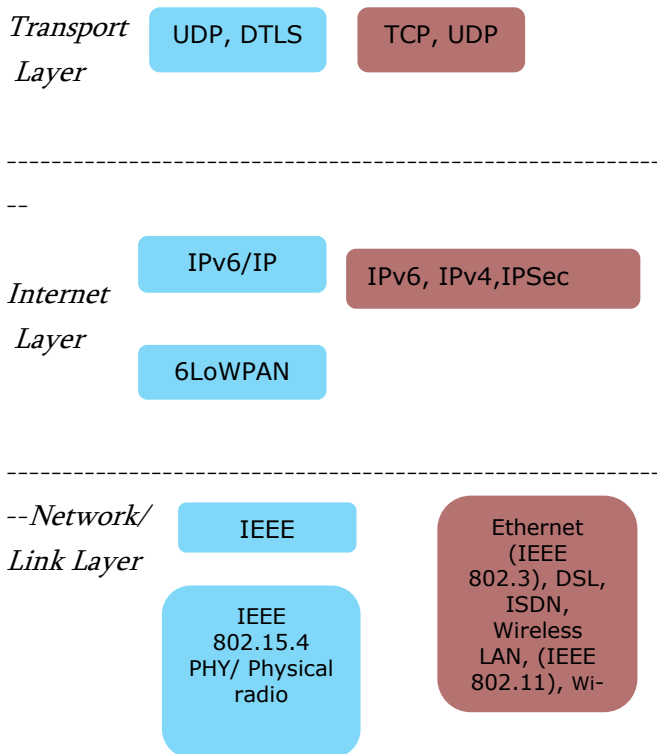


Fig 4. Standardized IOT Protocols

III. RESULTS AND DISCUSSION

Applications of IOTs

There are various IOT application scenarios identified as per survey conducted by IOT-1 project in 2010[7] in various domains like smart home, smart city, retail, agriculture, health care, environment and energy. The following survey was based on 270 responses from 31 countries. Among them the most attracted scenarios are: smart homes, healthcare, smart city, transportation[7]. So, in this paper we are going to get a brief idea about the applications like smart home, health care, intelligence security system.

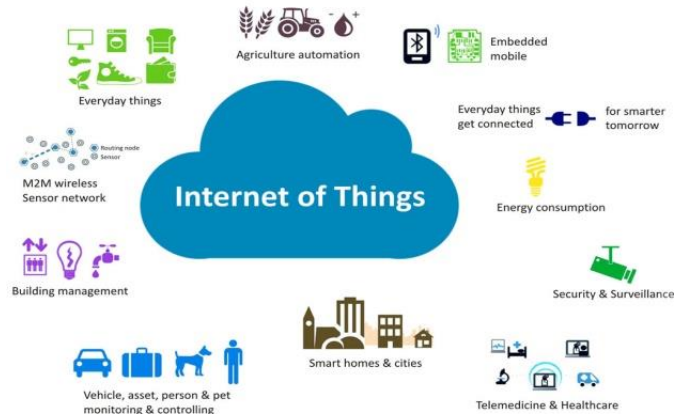


Fig 5: IOT Application domains

A. Smart Environment:

Smart structures, smart houses, and Smart city are incorporated under Smart Environment. Smart houses and smart cities are emerging in response to an increasingly more urbanized world dealing with scarce assets and a desire to enhance power efficiency. Smart cities [9] will assist deal with congestion and energy waste, whilst additionally assisting to enhance nice of life. Smart homes[8] will benefit from the IOT to improve strength efficiency, security and comfort thanks to the introduction of intelligent, connected devices.

For example, the smart house is the thought were each electronics device such as washing machine, refrigerator, oven etc. can be manipulated by remotely or by programmatically. Additionally by virtue of smart house systems, windows, home ventilation, doors, lighting, air-con etc. may be controlled remotely. There are several alternative applications already exist. During this regard however the thought is to boost the comfort level of the human inside the building premises. Due to the advancements of IOT technology, the metropolitan cities and municipalities are interconnected with technology to increase the infrastructure installation and efficiency, by improving reliability and quick response of emergency services within the low cost.

So, in future many cities will adopt the smart infrastructure. The main points of smart cities are cost, less resource utilization and efficiency. The IEEE Standards Association says [10] of smart cities "As world urbanization continues to grow and therefore the total population expected to double by 2050, there exists associated augmented demand for intelligent, property environments that scale back environmental impact and over a human's prime quality life as a result of a smart city brings along technology, government and society to modify a smart economy, good quality, a smart surroundings, good individuals, good living and good governance.

B. Environmental Monitoring:

Environmental monitoring like air pollution, forest fire detection, landslide or avalanche prevention /forest fire detection and earthquake early detection etc. can be identified effectively by using IOT technology. The IOT technology helps in making decision by integrating low level systems information with central or global system data. Using IOT environmental monitoring applications we can protect the environment by monitoring air or water quality, soil or atmospheric conditions and even include areas like monitoring the movements of wildlife and their habitats with the help of sensors in monitoring applications. The uses of IOT are: wireless networks are used to monitor and report pollution through sensors, smart-farming with over 70% cultivable land in India [10]. The usage of IOT can greatly benefit the farmers in not, only controlling production also in soil protection. The quality of the water is checked in the ocean by using sensors connected to a buoy and mooring device that sends information via GPRS network. Another critical usage with IOT technology is energy efficiency where ICT-empowered atmosphere relief procedures could diminish worldwide environmental change 16.5% by 2020[10] contrasted with current endeavors.

C. Health Care:

Health care is one of the emerging domains of IOT with many medical applications like fitness programs, health monitoring, chronic disease, elderly care [12]. The important potential application is treatment and medication at home with the help of medical providers. The smart things or objects constituting to the core of medical services are sensors, diagnostic and imaging. The emergence of IOT-based health care services are necessary to increase with the low cost, increase the standard of life, and enrich the user's expertise.

In [12] authors enhance the IOT frame and protocols for health care services. They use this particular services for IOT health care applications like blood pressure monitoring, glucose level sensing, body temperature, electrocardiogram, oxygen saturation monitoring, wheelchair management etc. This [12] paper surveys various aspects of IOT-based health-care technologies and presents different health care network architectures and platforms that support access to the IOT backbone and facilitate medical knowledge transmission and reception

D. Social Networking:

Internet of things (IOT) is currently changing into a brand new revolution once IoT in IT domain. It's the mix of internet technology and machinery industry. The essential plan of this idea is that the pervasive presence around us of a variety of things or objects like Radio-frequency identification (RFID) tags, sensors, actuators, mobile phones, etc.-that through unique addressing schemes, are able to communicate with one another and cooperate with neighbours to reach common goals[13]. The author proposed on the application of object oriented method in social-IOT and also presents a human being centred social-IOT construction method. The concept of the web of things is also important in this regard that plays a vital role in social networking innovations.

E. Security and Surveillance:

The aim of the IOT technology is to provide security and privacy using IOT and automation which is being expanded because of straight forwardness through smart phones, internet and wireless communication. IOT is a system of interconnected computing devices with unique identifiers and have the ability to transfer the data over the network[14],to fulfill the requirements of users regarding surveillance of their smart homes an IOT based smart surveillance system has been designed. It has countless applications and can be used in different environments and scenarios. When ant motion has been detected in the surveillance area the video is recorded, an email alert and SMS notifications are sent to the user informing about the motion detection. so, with the help of Wi-Fi or internet the user can view the video from the remote location itself.

5. Research Challenges and Opportunities in IOT:

The concept of IOT is currently being powerfully influenced in computing and network ubiquity. The developments within the next generation of internet are considered at all levels including United Nations[15]. "We have headed into a new era of ubiquity, where the users of the web are counted in billions, and wherever humans could become the minority as generators and receivers of traffic. Changes brought by the internet are dwarfed by people who prompted by the networking of everyday objects"[16].The importance of IOT in future are often absolutely pictured with the assistance of Fig.6[16].

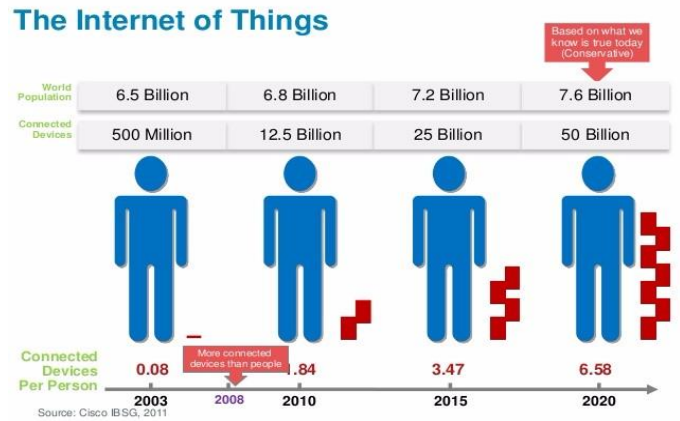


Fig 6. Comparison of Humans and Connected Devices

A report titled "The Internet of things Business Index: A quiet revolution gathers pace"[11], additionally found that 30% of business leaders feel that the IOT will unlock new revenue opportunities, where as 29% believe it'll inspire new operating practices, and 23% believe it'll eventually change the model of how they operate[17].

The challenges of IOT is summarized as:Though development of the many IOT primarily based systems are reported that there are many design challenges faced by the developers and engineers[19].



Fig 7: Security challenges facing IOT

Data Integrity: It is a interlinked ecosystem with billions of devices connected through IOT. So, change in any single data point can lead in

manipulation of complete information that is exchanged between the sensor and the main server. To ensure data integrity decentralized distributed ledger and digital signatures ought to be enforced.

Encryption Capabilities:Data must be encrypted and decrypted to protect it from attackers over the network. IOT sensors are lacking with the capability of the continuous process of encryption. Separate networks with segregated devices and firewalls are used to overcome the brute force attack.

Privacy Issues: IOT is all concerning about the exchange of knowledge among numerous platforms, devices and consumers. The smart devices gather knowledge from variety of reasons like rising potency and knowledge, higher cognitive process, providing higher service, etc., . Thus, the top purpose of knowledge shall be utterly secured and safe-guarded.

Common Framework:As there's no common framework for maintaining security and privacy all manufacturers are using their own ways. So, as a suggestive method the individual efforts can be utilized in a effective manner to make sure that reusability of code can be achieved through a common framework.

Automation:As the enterprises got to contend with a lot of variety of IOT devices it becomes troublesome to handle huge quantity of user information. So, one error in an exceedingly formula or algorithm would bring down the whole infrastructure of the information.

Updating: Managing and updating of enormous amount of information collected from numerous devices can be done mechanically. There should be track of the accessible updates and also the same should be applied to all the numerous devices. So, this becomes long and sophisticated method because

if any mistake happens with in the method than that shall result in loopholes with in the security later.

Security:Investing in security infrastructure is the first priority because security at each and every layer is suggested for IOT devices because it involves millions data information from sensors. From embedded system software to web applications each layer ought to be security intact. So, with a set of heterogeneous devices, security becomes advanced.

The challenges of IOT can be summarized as:

Development of rechargeable batteries for various electronic devices [19] is one of the opportunity available in IOT technology. The industrial IOT also includes high-stake opportunities in the fields like defence, automotive, aerospace, energy, healthcare [12]. I think the biggest opportunities lie outside some of the "flashy" consumer-level devices like wearable's, thermometers and smart refrigerators [20].

IV. CONCLUSION

This paper has shortly delineated different issues towards sensible realization of Internet of Things (IOT). A lot of research is going on towards technical implementation of IOT to give a positive impact on the society. At the same time many issues like security, authentication, information storage are rising in IOT technology which needs at most care. The main features that differentiate IOT security issues from the traditional ones are the heterogeneous large scale objects and networks which makes much more difficult to deal with. In this paper , we have discussed about different application domains and various security issues related to every layer in architecture of IOT. This paper will also help the researchers and practitioners to understand potential research challenges of IOT that will become research trends in future.

V. REFERENCES

- [1]. Cisco white papers, "The internet of Things"- How the next Evolution of the Internet Is Changing Everything, by Dave Evans, April 2011.
- [2]. <http://www.channelfutures.com/msp-501/iot-past-and-present-the-history-of-iot-and-where-its-headed-today>.
- [3]. Mohamed Abomhra, "Security and Privacy in the Internet of Things:Current Status and Open Issues" in ICEBI-10, Advances in Intellegant Systems Research, ISBN, vol.978,pp.90-78 677,2010.
- [4]. J.Sathish kumar, "A Survey on Internet of Things: Security and Privacy Issues" International Journal of Computer Applications(0975-8887) Volume90-No 11, March 2014.
- [5]. <https://www.milesweb.com/blog/hosting/cloud/importance-cloud-internet-things/>
- [6]. <https://www.mphasis.com/content/dam/mphasis-com/global/en/downloads/POV/Mphasis-Digital-POV-Emerging-Open-Standard-protocol-stack-for-IoT.pdf>.
- [7]. O.Vermesan, p.Friess, and A.Furness, The Internet of Things 2012, By New Horizons, 2012.[Online].Available: http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2012_WEB.pdf.
- [8]. Habib Ur Rehman, "Future applications and research challenges of IOT" International Conference on Information and Communication technologies (ICICT) Electric ISBN:978-1-5386-2186-8, March 2018.
- [9]. Vandan Sharma, Ravi Tiwari, "A review paper on IoT & it's smart Applications" International Journal of Science Engineering and Technology Research(IJSETR), Volume 5,Issue2,February 2016.
- [10]. <https://www.iotevolutionworld.com/smart-home/articles/441882-internet-things-smart-cities.htm>,<https://telecom.economictimes.indiatimes.com/tele-talk/how-iot-is-playing-a-key-role-in-protecting-the-environment/2414>.
- [11]. Y.YIN, Yan Zeng and Xing Chen," The Internet of Things in Healthcare: An Overview, "Journal of Industrail Information Integration, Vol 1 2016.
- [12]. Riazul Islam, S.M, Daehan kwak, Humaun kabir, Mahmud hossain and kyungsup kwak, "The Intenet of Things for Health Care:A Comprehensive Survey. IEEE Access, Volume 6 2015.
- [13]. D.Giusto, A.lera,G.Morabito and L.Atzori, "The Internet of Things", Springer 2010,ISBN: 978-1-4419-1673-0
- [14]. Gunnemeda Leela Krishna et.al, "IoT Based Smart Surveillance System" International Journal of Advance Research and Development(IJARD),Vol 3,Issue 3 2018.
- [15]. Mukhopadhyay,S.C,"Internet of Things: Smart Sensors, Measurement and Instrumentation, DOI:10.1007/978-3-319-04223-7.
- [16]. https://en.wikipedia.org/wiki/Internet_of_things Accessed on 27th July 2019.
- [17]. https://www.arm.com/files/pdf/EIU_Internet_Business_Index_WEB.pdf Accessed on 27th July 2019.
- [18]. <https://www.colocationamerica.com/blog/security-challenges-of-iot> Accessed on 27th July 2019.
- [19]. Zhang, Michael Cheng yicho, Chia_wei wang, chia_wei Hsu, Chong-kauan Chen and shiuhpyng shieh, "IoT Security: Ongoing Challenges and Research Opportunities.2014 7th International Conference on Service Oriented Computing and Applications,DOI:10.1109/SOCA.2014.58
- [20]. <https://www.globalsign.com/en/blog/internet-of-things-challenges-and-opportunities>

Cite this article as :

Uppuluri Sirisha, Dr. G. LakshmeEswari, "A Survey on Internet of Things : Applications and Layered wise Security Issues", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 6, pp. 171-180, November-December 2019. Available at doi : <https://doi.org/10.32628/CSEIT195624>
Journal URL : <http://ijsrcseit.com/CSEIT195624>