A Survey on Internet of Things: Related Future Technologies, Applications, Challenges and Security Risks

Rachita Kansal
Assistant Professor
Department of Computer Science & Engineering
AKMV Shahabad Markanda, India

Abstract - Internet of Things (IoT) is an important technology that promises a smart human being life, by allowing a communications between objects, machines and every things together with people. IoT represents a system which consists of things in the real world, and sensors attached to or combined to these things, connected to the Internet via wired and wireless networks. The concept of Internet of Things (IoT) is based on a layered architecture consisting of many different layers. Each of the layer includes the application of a range of various technologies for the data transmission, processing and storage. The IoT sensors can use various types of connections such as Wi-Fi, Bluetooth, and ZigBee, in addition to allowing wide area connectivity using many technologies such as GSM, GPRS, 3G, and LTE. IoT enabled things will share information about the things and the surrounding environment with people, software systems and other machines. By the technology of the IoT, the world will become smart in many aspects, since the IoT will provides a means of smart cities, smart healthcare, smart homes and building, in addition to many important applications such as smart energy, transportation, waste management and monitoring. In this paper we review a concept of many IoT technologies, applications in addition to the challenges that facing the implementation of the IoT and as well as security risks on the basis of type of use of IoT technology will be proposed.

Keywords - Internet of Things, Applications, Future Technologies, Smart Cities, Smart Environment, Smart Energy, Smart Manufacturing, Smart Healthcare, Security Risk assessment, Data protection.

---

1. INTRODUCTION

The Internet of Things (IoT), sometimes referred to as the Internet of Objects that can change everything including ourselves. The Internet has an impact on education, communication, business, science, government, and humanity [1]. The Internet is one of the most important and powerful creations in all of human history and now with the concept of the internet of things, internet becomes more favorable to have a smart life in every aspects[1].Internet of Things is a latest technology of the Internet accessing. By the Internet of Things, objects recognize themselves and obtain intelligence behavior by making related decisions. Figure 1 reviews that with the internet of things, anything's will able to communicate to the internet at any time from any place to provide any services by any network to anyone. This concept will create new type of applications which can involve smart vehicle and the smart home, to provide many services such as notifications, security, energy saving, automation, communication, computers and entertainment. The growing role of the Internet of Things (IoT) concept is proved by its applications in the number of areas such as the development of smart cities, the management of energy resources and networks, mobility, transport, logistics, smart healthcare, energy saving etc.

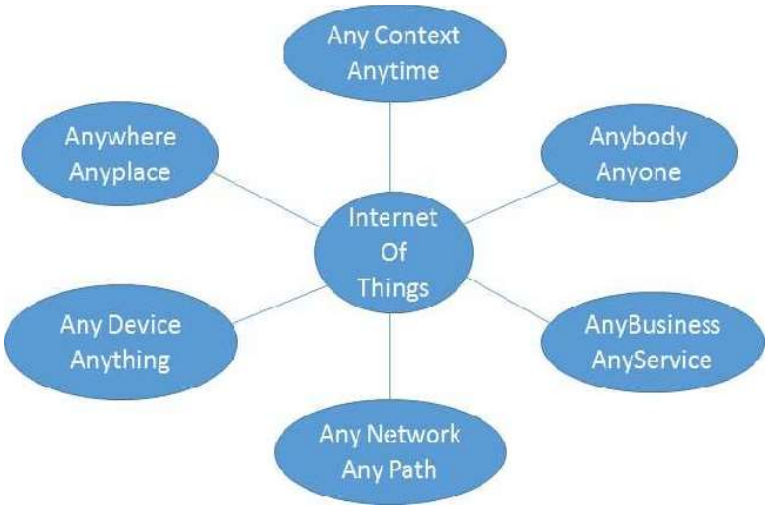

Figure 1

The increase in the application and the importance of this concept results in an increasing number of diverse data being processed, stored and transmitted in different environments.In the near future, storage and communication services will be highly pervasive and distributed: people, machines, smart objects, surrounding space and platforms connected with wireless/wired sensors, M2M devices, RFID tags will create a highly decentralized resources interconnected by a dynamic network of networks. The aim of this paper is to present the internet of things Applications, Future Technologies, and challenges and to examine security aspects of a particular layer of the IoT architecture and development of appropriate protection methods of the most vulnerable layers.

2. INTERNET OF THINGS STANDARDIZATIONS AND PROTOCOLS

By the 2020 around 50 to 100 billion things will be connected electronically by internet network according to recent analysis. Figure 2 shows the growth of the things connected to the internet from 1988 to 2020. The Internet of Things (IoT) will provide a technology to create the means of smart tasks for machines to communicate with one another and with many different types of information. The success of IoT depends on standardization, which provides interoperability, compatibility, reliability, and many other effective operations on a global scale. The IoT standards' design is required to consider the efficient use of energy and network capacity, as well as respecting other constraints such as frequency bands and power levels for radio frequency communications. IEEE Standards Association (IEEE-SA) developed a number of standards that are related to environment needs for an IoT. The IEEE-SA has approximately 900 active standards and more than 500 standards under development. In its research into IoT, it has identified over 140 existing standards and projects that are relevant to the IoT.

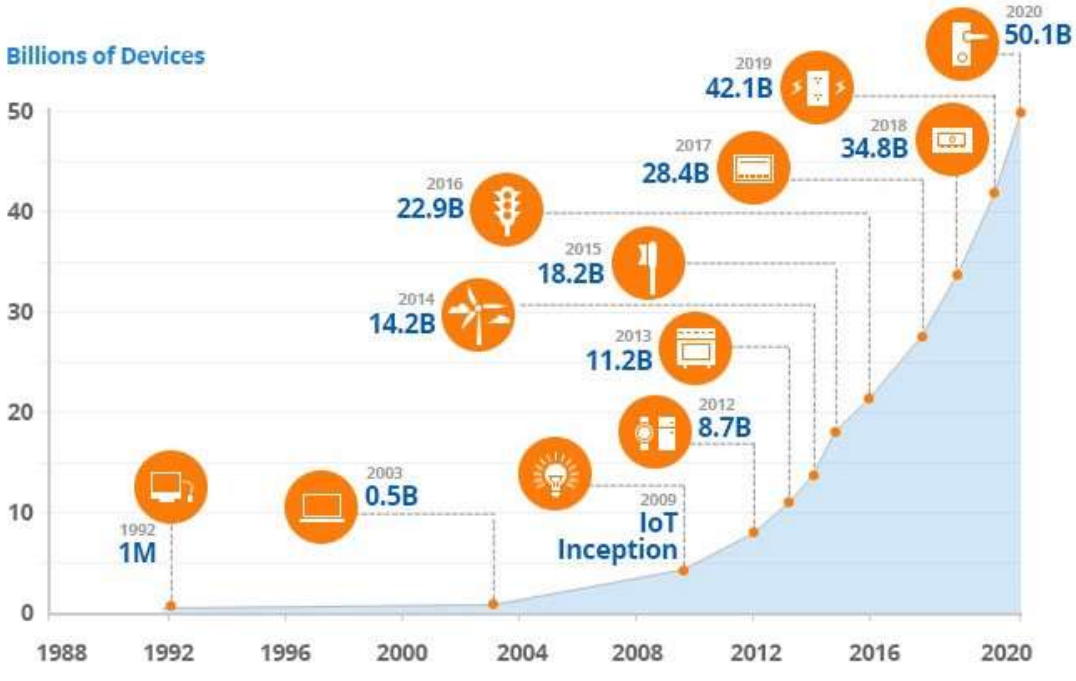

Figure 2

ETSI produces globally applicable standards for information and communications technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies. These standards are considered as one of the basic standards of IoT, because it associate with M2M technology which is one of the basic techniques of IoT.

3. INTERNET OF THINGS AND RELATED FUTURE TECHNOLOGIES

Many new technologies are related to IoT to prove the enhancement of wired and wireless control, communication and IT technologies together which are responsible for connecting several subsystems and things which operate under a unified fixed platform on which they are controlled and managed smartly.

A. Cloud Computing

The two worlds of Cloud and IoT have seen a rapid and independent evolution in past few years. These worlds are very different from each other, but their characteristics are often complementary in general, in which IoT can benefit from virtually unlimited and unbounded capabilities of cloud to compensate its technological constraints for example storage, processing, retrieval and communication. Cloud can offer an effective solution for IoT service management and composition .On the other hand, cloud can benefit from IoT by extending its scope to deal with real world things in a more distributed and dynamic manner, and for delivering new invented services in real life scenarios. In many cases, Cloud can provide the intermediate layer between the things and the applications, hiding all the complexity and functionalities necessary to implement these applications. This will impact future application development, where information gathering, processing, and transmission will generate new challenges, especially in a multi cloud environment or in fog cloud.

B. Big Data

Due to the rapid expansion of the networks now-a-days, the number of devices and sensors in networks are increasing more and more in the physical environment which will change the information networks, services and applications in various domains. The expectations in the next year's shows that around 50 billion devices will generate large data volumes from many applications and services in a variety of areas such as smart grids, smart homes, healthcare, automotive, transport, logistics and environmental monitoring. The related technologies and solutions that enable integration of real world data and services into the current information networking technologies are often done under the term of the Internet of Things (IoT) .The volume of data on the Internet and the Web is still growing, and everyday around 2.5 quintillion bytes of data is created and it is estimated that 90% of the data today was generated in the past two years.

C. Security and Privacy

Due to the fact that IoT applications are able to access the multiple higher level domains and involve multiple ownership regimes, there is a need for a trust framework to enable the users of the system to have confidence that the information and services being exchanged are trustworthy. The trust framework needs to be able to deal with humans and machines as users, for it needs to convey trust to humans and needs to be robust enough to be used by machines without denial of service. The IoT requires a variety of access control schemes to support the various authorization models that are required by users. New techniques and approaches for example like machine learning, are required to lead to a self-managed IoT. Cryptographic techniques is also very important in IoT based systems to enable a means of data protection to be stored ,processed and shared, without the information content being accessible to other parties.

D. Distributed Computing

Distributed computing uses groups of networked computers for the same computational goal. Distributed Computing has several common issues with concurrent and parallel computing, as all these three fall in the scientific computing field. Nowadays, a large amount of distributed computing technologies coupled with hardware virtualization, service oriented architecture, and autonomic and utility computing have led to cloud computing. Internet of Things with distributed computing represents a vision in which the Internet extends into the real world embracing everyday objects. Physical items are no longer disconnected from the virtual world, but can be remotely controlled and can act as physical access points to Internet services.

E. Fog Computing

Fog computing is related to the edge computing in the cloud. In contrast to the cloud, fog platforms are dense computational architectures at the network's edge. Characteristics of such platforms reportedly include low latency, location awareness and use of wireless access. While edge computing or edge analytics may exclusively refer to perform analytics at devices that are on, or close to, the network's edge, a fog computing architecture would perform analytics on anything from the network center to the edge. IoT may more likely be supported by fog computing in which computing, storage, control and networking power may exist anywhere along the architecture, either in data centers, the cloud, edge devices such as gateways or routers, edge equipment itself such as a machine, or in sensors .

4. INTERNET OF THINGS APPLICATIONS

Internet of things provided many applications in human life which makes life easier, safe and smart. There are many applications of IOT such as smart cities, homes, transportation, energy and smart environment.

1. Smart home

Smart Home ranking is highest among Internet of Things application on all measured channels. On an average, More than 60,000 people currently search for the term "Smart Home" each month. This is not a surprise. The IoT Analytics company database for Smart Home includes more than 256 companies and startups. More companies and startups are active in smart home than any other application in the field of IoT. The total amount of funds needed for Smart Home startups currently exceeds $2.5bn. This list includes prominent startup names such as Nest or AlertMe as well as a number of multinational corporations like Philips, Haier, or Belkin.

2. Wearables

Wearables also remains a hot topic in field of IoT. As consumers eagerly waited for the release of Apple's new smart watch in April 2015, there are plenty of other wearable innovations to be excited about: like the Sony Smart B Trainer, the Myo gesture control, or LookSee bracelet. Of all the IoT startups, wearables maker Jawbone is probably the one with the biggest funding till date. It stands at more than half a billion dollars!

3. Smart City

Smart city includes a wide variety of use cases i.e. from traffic management to water distribution, waste management, urban security and environmental monitoring. Its popularity is achieved by the fact that many Smart City solutions promise to alleviate real pains of people living in cities these days. IoT solutions in the area of Smart City solve traffic congestion problems, reduce noise and pollution and help make cities safer.

4. Smart grids

Smart grids is a special one in IOT. A future smart grid promises to use information about the behavior of electricity suppliers and consumers in an automated fashion to improve the efficiency, reliability, and economics of electricity. 41,000 monthly Google searches highlights the concept's popularity. However, the lack of tweets (Just 100 per month) shows that people don't have much to say about it.

5. Industrial internet

The industrial internet is also one of the special Internet of Things applications. While many market researches such as Gartner or Cisco see the industrial internet as the IoT concept with the highest overall potential, its popularity currently doesn't reach the masses like smart home or wearables do till now. The industrial internet however has a lot going for it. The industrial internet gets the biggest push of people on Twitter (~1,700 tweets per month) compared to other non-consumer-oriented IoT concepts.

6. Connected car

The connected car is coming up slowly. Owing to the fact that the development cycles in the automotive industry typically take 2-4 years, we haven't seen much buzz in the field of connected car yet. But it seems we are getting there. Most large auto makers as well as some brave startups are working on connected car solutions. And if the BMWs and Fords of this world don't present the next generation internet connected car soon, other well-known giants will: Google, Microsoft, and Apple have all announced connected car platforms.

7. Connected Health (Digital health/Telehealth/Telemedicine)

Connected health remains the sleeping giant of the Internet of Things applications. The concept of a connected health care system and smart medical devices bears enormous potential, not just for companies also for the well-being of general people. Connected Health has not reached the masses yet. Prominent use cases and large-scale startup successes are still to be seen in the area of smart health.

8. Smart retail

Proximity-based advertising which is a subset of smart retail is starting to take off. But the popularity ranking shows that it is still a niche segment. One LinkedIn post per month is nothing compared to 430 for smart home.

9. Smart supply chain

Supply chains have been getting smarter from some years already. Solutions for tracking goods while they are on the road, or getting suppliers to exchange inventory information have been on the market from years. So while it is perfectly logic that the topic will get a new push with the Internet of Things, it seems that so far its popularity remains limited.

10. Smart farming

Smart farming is an often overlooked business-case for the internet of Things because it does not really fit into the well-known categories such as health, mobility, or industrial. However, due to the remoteness of farming operations and the large number of livestock that could be monitored the Internet of Things could revolutionize the way farmers work. But this idea has not yet reached large-scale attention. Nevertheless, one of the Internet of Things applications that should not be underestimated. Smart farming will become the important application field in the predominantly agricultural-product exporting countries.

11. Business Services

A facility services company uses their multi-device IoT software to enable support personnel to receive alerts about service issues and take immediate action. By aggregating data from thousands of sensors in devices like coffee machines, soap dispensers, paper towel dispensers and mouse traps rather than doing manual checks, the application has significantly cut costs and improved service levels.

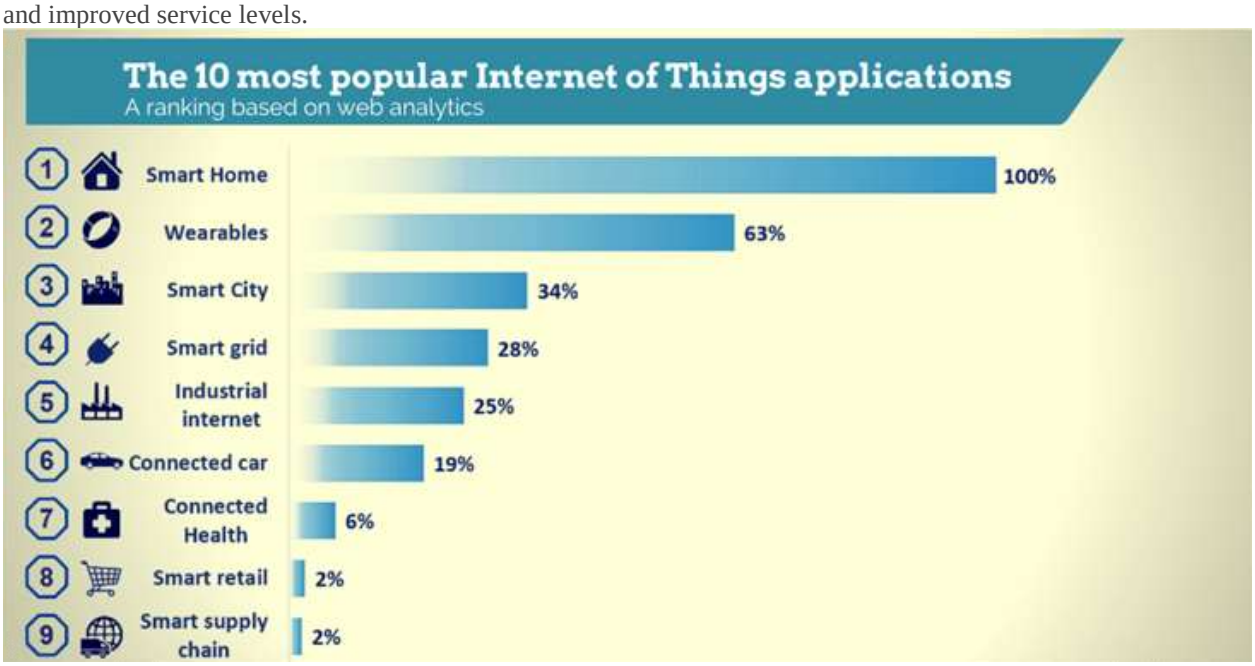

Figure 3

4. INTERNET OF THINGS CHALLENGES

There are some challenges to the applications of the Internet of Things concept in cost of implementation. The expectation that the technology must be available at economic cost with a large number of objects. IoT faced many challenges, such as:

 Scalability: Internet of Things has a big concept than the conventional Internet of computers because of things that are cooperated within an open environment. Basic functionality such as communication and service discovery need to function equally efficiently in both small scale and large scale environment. The IoT requires number of new functions and methods in order to gain an efficient operation for scalability.

 Self-Organizing: Smart things should not be managed like computers that require their users to configure and adapt them to particular situations. Mobile things, which are often used, needs to establish connections spontaneously, and are able to organize and configure themselves to suit their particular environment.

 Data volumes: Some application scenarios of the internet of things are involved in infrequent communication, and gathering information's form sensor networks, or form logistics and large scale networks, will collect a huge volumes of data on central network nodes or servers. The term represent this phenomena is big data which requires many operational mechanism in addition to new technologies for storing, processing and management.
 Data interpretation: To support the users of smart things, there is a need to interpret the local context determined by sensors as accurately as possible. For profit of service providers, the disparate data that will be generated need to be able to draw some generalizable conclusions from the interpreted sensor data.
 Interoperability: Each type of smart objects in Internet of Things have different information, processing and communication capabilities. Different smart objects would also be subjected to different conditions such as the energy availability and the communication bandwidth requirements. To facilitate communication and cooperation of these objects, common standards are required.

 Automatic Discovery: In dynamic environments, suitable services for things must be automatically identified, which requires appropriate semantic means of describing their functionality.
 Software complexity: A more extensive software infrastructure will be needed on the network and on background servers in order to manage the smart objects and provide services to support them. That because the software systems in smart objects will have to function with minimal resources, as in conventional embedded systems.
 Security and privacy: In addition to the security and protection aspects of the Internet such in communications confidentiality, the authenticity and trustworthiness of communication partners, and message integrity, other requirements would also be important in an Internet of Things. There is a need to access certain services or prevent from communicating with other things in IoT and also business transactions involving smart objects would need to be protected from competitors' prying eyes.
 Fault tolerance: Objects in internet of things is much more dynamic and mobile than the internet computers, and they are in changing rapidly in unexpected ways. Structuring an Internet of Things in a robust and trustworthy manner would require redundancy on several levels and an ability to automatically adapt to changed conditions.
 Power supply: Things typically move around and are not connected to a power supply, so their smartness needs to be powered from a self-sufficient energy source. Although passive RFID transponders do not need their own energy source, their functionality and communications range are very limited. Hopes are pinned on future low power processors and communications units for embedded systems that can function with significantly less energy. Energy saving is a factor not only in hardware and system architecture, but also in software, for example the implementation of protocol stacks, where every single transmission byte will have to justify its existence.
 Wireless communications: From an energy point of view, established wireless technologies such as GSM, UMTS, Wi-Fi and Bluetooth are far less suitable; more recent WPAN standards such as ZigBee and others still under development may have a narrower bandwidth, but they do use significantly less power.

5. THE ARCHITECTURE OF IOT ENVIRONMENT

IoT architecture concept is based on an open model using open protocols in order to support existing network protocols. Generic, layered architecture of IoT concept consists of four basic layers (perception layer, network layer, middleware layer and the application layer), shown by Figure 4.

Perception layer consists of two main functionalities, data collection and collaboration between the elements of the same layer. The **network layer** consists of two sublayers, access sublayer with the role of collecting the data from perception layer and sending it to the Internet sublayer. Internet sublayer is the backbone of IoT environment and its main task is the transfer of data to the next layer. **Middleware layer** is responsible for data collecting, its filtering, transformation and the intelligent processing most commonly with the use of cloud computing data is passed to the next layer. A**pplication layer** which uses the given data in order to provide and present various services to the end user.

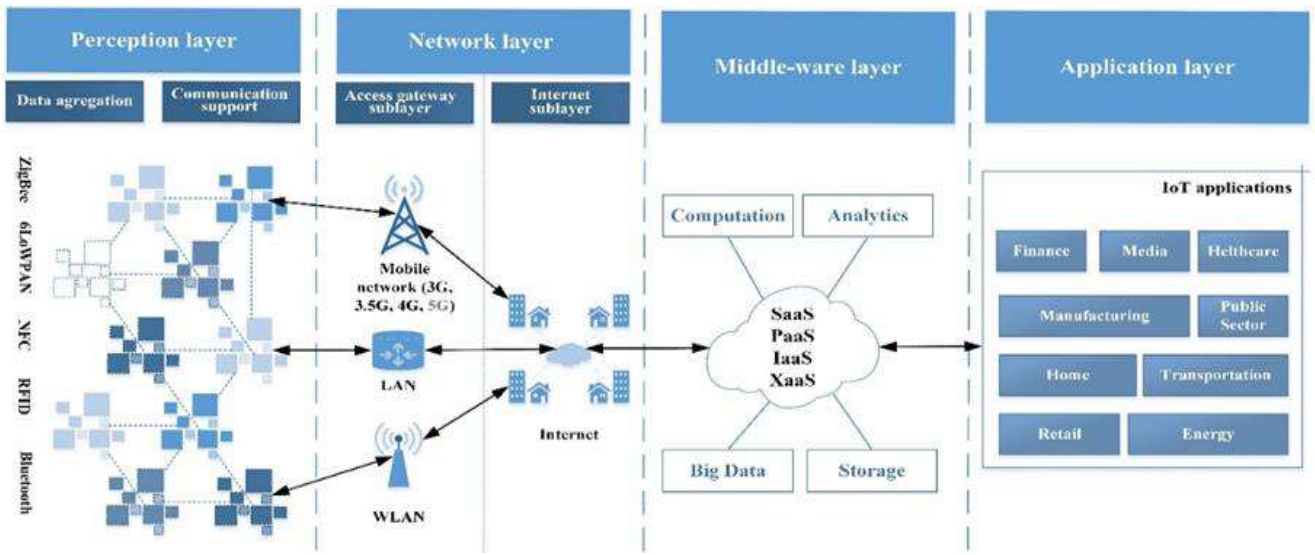

Figure 4

6. SECURITY ASPECTS OF THE IOT ARCHITECTURE LAYERS

The growing use of IOT system needs a powerful protection against all possible attacks and security risks. Hence security is needed at each layer of the IOT system; each layer either consists of devices, applications or networks as shown in IoT system architecture. Some classified security issues at each layer are as given below:

3.1.1 **Security at Perception Layer** Perception layer mainly includes: Smart card, Reader, RFID tag, Sensor network. Each of these devices has following risks which leads to be a security issue of IOT such as sensor attacks, sensor abnormalities and radio interference.

3.1.1.1 **Terminal security issues** For perception of things it needs a large number of terminals, terminals are used for real-time data collection which is to be presented to the user. This process needs an authentication and data integrity. Due to the wireless nature of communication, IOT can face threat from the hackers, virus attacks etc. The main problems existed in perception terminals include leakage of confidential information, terminal virus, copying and other issues.

3.1.1.2 **Sensor network security issues** The sensor nodes are responsible for data transmission, data acquisition, integration and collaboration. As they operate on their own battery with less security protection, they can face complex security issues as follows:

- Invoking Malicious Codes: Malicious programs such as worm which does not require any parasitic file, can easily affect the wireless and sensor network, hence it will be very difficult to detect the malicious code and act accordingly.
- Defect of the tag: Due to the limited cost of tag, it is not possible to provide enough security which leads to illegal use of legal reader due to which an attacker can easily get the information on tag and can illegally access RFID system without any authorization by counterfeiting. Any rewritable tag can be copied, decoded or fabricated by the attacker.

3.1.2 **Security at Network layer** Network layer mainly including Computers, Wireless or wired network, faces security issues such as network content security, hacker intrusion, and illegal authorization.

3.1.2.1 **Data transmission security issue** The goal of network layer is to transmit information, the information need to be transmitted securely. 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. In wireless networks, nodes can move freely, they can join or leave the network at any time without any prior authentication. This makes wireless networks to be more malicious or vulnerable for the security concern. 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.

3.1.3 **Security aspect of the middleware layer**

The middleware layer is based on cloud computing because of its benefits, such as delivery of computing resources as a service to end users, flexibility, scalability, etc. This makes it suitable for processing large amount of data collected on the perception layer and the presentation of processed data to end users through a variety of applications. Due to the rapid evolution and a high acceptance degree, this concept has a large number of threats and vulnerabilities

that inherit the middleware layer of the IoT concept based on cloud computing . The fact that this layer accumulates all the data collected on the perception layer raises the issues of data security. An additional problem is the public or hybrid cloud computing model, where a single physical server can contain multiple virtual machines from different IoT service providers or even the presence of malicious users with the possibility to gain unauthorized access to other virtual machines and to manipulate stored data.

3.1.4 **Security at Application layer** Application layer mainly includes the intelligent devices for effective decision making. Each of these has some vulnerability which leads to be an issue of the security of IOT.

3.1.4.1 **Application safety issues** Application layer mainly contains a variety of applications for example, industrial monitoring, smart grid, monitoring services, or any other intelligent system. The main security problem can be its own design flaws that can attract any attacker to attack. Malicious code or software vulnerabilities can be introduced in such defected systems. Another issue can be the integration of various areas of techniques and business needs which can cause a bottleneck for the massive data processing and on operation control this can lead to the security issues of reliability and safety for IOT. Some of the issues could be privacy protection technology, database access control, protection technology of secure electronic products, information leakage tracking technology and intellectual property of software.

CONCLUSION

Internet of things is a new technology which provides many applications to connect things to things and human to things through the internet. Each object in the world can be identified, connected to any other object through internet. Some commonly used networks and technologies of communication used in building the concept of internet of things are mobile computing, RFID, wireless sensors networks, and embedded systems, in addition to many algorithms and methodologies to get management of processes, storing data, and security issues. Internet of things is facing two major challenges in order to guarantee seamless network access; the first issue relates to the fact that today different networks coexist and the other issue is related to the big data size of the IoT. Other current issues, such as address restriction, automatic address setup, security functions such as authentication and encryption, and functions to deliver voice and video signals efficiently will probably be affected in implementing the concept of the internet of things but by technological developments these challenges will be overcome soon. The internet of things promises future new technologies when related to cloud, fog and distributed computing, big data, and security issues. By integrating all these issues with the internet of things, smarter applications will be developed soon. This paper surveyed some of the most important applications of IoT with particular focus on what is being actually done in addition to the

challenges that are facing by the world. According to estimates, by means of this concept 50 billion devices will be connected by 2020 which places heavy demands and challenges in maintaining the required safety level of such an environment. This paper also analyzed the security aspects for each layer of the IoT architecture, and based on that, the proposal of risk classification of the IoT architecture layers has been made. By the analysis of security vulnerabilities, it was concluded that the biggest security risk is in a perception layer of the IoT architecture due to the specific limitations of devices and the transmission technology used at this layer, followed by the middleware layer based on cloud computing and inherited vulnerabilities of that concept. The highest level of risk of the IoT concept application was determined for the financial, manufacturing and multimedia sector due to the largest increase of its usage in the last few years. The results presented in this research provide new knowledge of IoT technologies, applications, challenges and security risks in the IoT environment.

References

[1] Zeinab Kamal Aldein Mohammed, Elmustafa Sayed Ali Ahmed. Internet of Things Applications, Challenges and Related Future Technologies. World Scientific News WSN 67(2) (2017) 126-148 EISSN 2392-2192.
[2] Ivan Cvitić, Miroslav Vujić, Siniša Husnjak, CLASSIFICATION OF SECURITY RISKS IN THE IOT ENVIRONMENT, INTERNATIONAL SYMPOSIUM ON INTELLIGENT MANUFACTURING AND AUTOMATION, 26TH DAAAM
[3] Mayuri A. Bhabad, Sudhir T. Bagade, Internet of Things: Architecture, Security Issues and Countermeasures, International Journal of Computer Applications (0975 – 8887) Volume 125, September 2015
[4] M. A. Ezechina, K. K. Okwara, C. A. U. Ugboaja. The Internet of Things (Iot): A Scalable Approach to Connecting Everything. *The International Journal of Engineering and Science* 4(1) (2015) 09-12.
[5] http://www.meraevents.com/event/iot-workshop
[6] http://www.nxp.com/assets/documents/data/en/white-papers/INTOTHNGSWP.pdf
[7] Saranya C. M., Nitha K. P., Analysis of Security methods in Internet of Things. *International Journal on Recent and Innovation Trends in Computing and Communication*, Volume 3, Issue 4; April 2015.
[8] Sapandeep Kaur, Ikvinderpal Singh. A Survey Report on Internet of Things Applications. *International Journal of Computer Science Trends and Technology* Volume 4, Issue 2, Mar - Apr 2016.
[9] S. Misra et al., Security Challenges and Approaches in Internet of Things. Springer Briefs in Electrical and Computer Engineering, 2016.
[10] Suwimon Vongsingthong and Sucha Smanchat. A Review of Data Management in Internet of Things. *KKU Res. J.* 2015
[11] https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-commercial-real-estate-intelligent-building-systems.html
[12] Grandinetti, Lucio. Pervasive Cloud Computing Technologies: Future Outlooks and Interdisciplinary Perspectives: Future Outlooks and Interdisciplinary Perspectives. IGI Global, 2013.
[13] http://standardsinsight.com/iot/iotworkshop
[14] Debasis Bandyopadhyay, Jaydip Sen. Internet of Things - Applications and Challenges in Technology and Standardization. arvix 9 may 2011
[15] http://www.academia.edu/3276195/Internet_of_Things_Applications_and_Challenges_in_Technology_and_Standardization
[16] Adam D. Thierer. The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation. 21 Rich. J. L. & Tech. 6 (2015).
[17] Patrick Guillemin, et al., Internet of Things Position Paper on Standardization for IoT technologies. European research cluster on the internet of things; January, 2015.
[18] Patrick Guillemin et al., Internet of Things standardization - Status, Requirements, Initiatives and Organizations. Conference: Internet of Things - Converging Technologies for Smart Environments and Integrated Ecosystems 2013.
[19] http://www.standardsuniversity.org/e-magazine/march-2016/security-and-iot-in-ieee-standards/
[20] Dr Ovidiu Vermesan, Dr Peter Friess. Internet of thing from research and innovation to market deployment, 2014 River Publishers.