International Journal of Scientific Research & Engineering Trends
Volume 6, Issue 1, Jan-Feb-2020, ISSN (Online): 2395-566X

Internet of Things: Survey on Future and Challenges

Research Scholar Ahmed Mohamed Maher, Mca, Ph.D, Asst. Prof. S.Suganya
Department of Computer Sciences Rathinavel Subramaniam
College of arts and science, Coimbatore, India

Abstract **- The computer science growth vary fast , and thanks to growing technology continuously One such concept is IoT (Internet of things) with which automation is no longer a virtual reality, IoT connects various non-living objects through the internet and enables them to share information with their community network to automate processes for humans and makes their lives easier. The paper presents the evaluation study of IoT,such as the technical challenges (connectivity , compatibility and longevity , standards , intelligent analysis and actions , security),the IoT architecture mainly requires two types of technologies: data acquisition technologies and networking technologies. Many technologies are currently present that aim to serve as components to the IoT paradigm. This paper aims to categorize the various technologies and challenges present that are commonly used by Internet of Things.**

Keywords- **IoT, Internet of Things, Security, Sensors.**

I. INTRODUCTION

The Internet of Things is a technology born out of a network. On the ends of the network are information sensing equipment and systems. These are devices that are able to obtain data or information from the physical world. Through a network, these objects can be connected to other such devices or other smart objects. Smart objects are able to analyze the data obtained from the information sensing equipment and make independent decisions. Imagine a shirt being able to tell the washer it is in what color it contains and any special care instructions it may have, and imagine the washer independently acting accordingly. The data can be stored in circuitry inside the shirt, or this shirt may refer the washer to an information database on the Internet. Thus, the communication over the Internet would include human-thing and thing-thing [3], [4].

The Internet of Things (IoT) is a synonym for the fully interconnected world [1]. It connects all the things with technology and makes a whole new separate world for them to interact with each other with the help of internet. IOT is not just a concept but can prove to be a revolution in advancing technology to change the lifestyles of humans altogether [2].

II. INTERNET OF THINGS PAST YEARS

The graph below depicts the growth of IoT over the years. In 1992, only 1,00,000 people were using IOT as a technology. Till 2003, the number grew to half a billion people. While 2009 marked the IOT inception, 2012 witnessed a sudden Increase in the usage of IOT where the people using IOT reached 8.7 billion, and there was no looking back. The number of users has been growing exponentially over the years reaching 28.4 billion in 2017. It is expected that the number will broaden to 50.1 billion by 2020 are described as shown in fig2.1. [5]

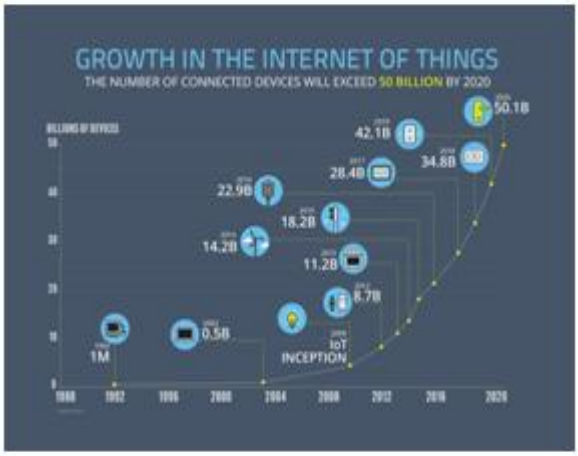

Fig.1. Survey of Growth of Internet of Things over past years.

III. WHEEL OF LIFE OF IOT INFORMATION

According to Red-hat Information Lifecycle cited in [12], Data that is generated and collected by sensors, actuators, human interfaces, control panels etc. are analyzed initially (field level) to produce information which can be used for further analysis and performing actions. further processed and examined to decide the desirable steps that need to be taken. The Information produced at this stage is used to trigger pre-defined business rules that

correspond to it. The Intelligence of the system takes the normal actions required to respond to the environment. The information gained from this experience is then summarized and sent to the knowledge base where it is stored and used for deep learning and analysis to draw new conclusions. New rules created here are sent to the Intelligence module to add to its accuracy, and more optimized tactical tools generated in the knowledge base are forwarded to the Information module to add to its expertise in analysis of data. The knowledge base is controlled, modified and amplified by experts of the domain the system belongs to.

IV. FUTURE OF IOT

The uncertainty and business risk is always present in any new technology. In case of IoT, it is observed that many of the dangers are physically not present somewhat they are distorted or misstated. While it will take time to develop the IoT vision fully, the building blocks to start the process are ready to be used.The major requirements such as - hardware and software assets are either available in a less quantity or some of them are under development; it is also a fact that: the security and confidentiality concerns of IoT devices are not properly addressed over past decade. It is a whole and sole responsibility of stakeholders to collaborate and carry out the open standards to make IoT reliable, secure and interoperable. Therefore, allowing secured services to be delivered seamlessly.Over the next few years IoT is expected to make over $19 trillion [6]. However, the problem associated with this : these 'things' have myths surrounding them, some of which are impacting how organisations develop the apps to support them.

1. **IoT and Sensors**
   The data produced by most sensors are not used efficiently. To help the technology evolve, 62% surveyed manufacturers believe that its functionality can be improved by advancing analytics features. More training on analytics tool was also thought to be one way by 45% people. More mobility, computing power and capacity to store data were also some factors mentioned by the manufacturers.
2. **IoT and Volume of Data**
   The production of data of IoT applications is extensive. It is the fact that: The total amount of data being generated by IoT applications is not required to be stored on cloud as it consists of a lot of useless chatter generated by devices in which no change in state is observed [7]. The most significant challenge in this context is the selective storage of data on a cloud so that there will not be a storage issue in the future use of IoT devices. It also concludes that appropriate and correct data will be given to the user while rest (garbage) data produced by IoT devices will be deleted appropriately.
3. **IoT and Datacenters**
   There is always constant argument that: Data in datacenters manages all the processes in IoT. It is a univocal fact that datacenter is entirely an essential factor for the IoT. We must also focus on the reliability of network which is used to run the IoT applications. High-speed Internet is equally important as its performance the functionalities like the reliable transmission of data, quick delivery of sensor data, fetching details from sensors to a cloud and vice versa [7].
4. **IoT as a Future Technology**
   IoT is an evolution in the multidisciplinary world. Microcontrollers and Microprocessors, sensors and networking devices are some of the basic building blocks of the IoT and these are in widespread use today. They have turned out to be all the more effective today, even as they get littler and more affordable to create.
5. **IoT and current interoperability standards**
   IoT in the long run included billions of interconnected devices over the internet. Looking at the boom of IoT, it will include numerous makers from around the globe producing numerous product categories [8].The term interoperability states that: All these devices must communicate trade information and perform closely synchronized manner. They should also show the task without compromising security standards and overall performance of IoT devices.
6. **IoT and privacy and security**
   Security and privacy are the main concerns while designing and developing IoT devices —and addressing these concerns must be a high priority. New technology often has scope for abuse, and it's smarter to solve the issue before it influences privacy and security, innovation or financial development. It is a responsibility of Manufacturers, standards organisations and policy-makers to address all the possible threats to the product. As a part of network layer security, manufacturers must think about the implementation of new security protocols that will be important to guarantee end-to-end transmission of delicate data.
7. **IoT and limited vendors**
   Open platforms have always been a proven way for developers and merchants to build innovative hardware with constrained spending plans and assets [13]. The behavior of IoT applications has heterogeneous nature. Hence it requires a wide variety of software and hardware. To manufactures all these IoT components, there must be a full number of vendors available in the market.
8. **IoT and Mobile Data**
   The effectiveness of the generation of data from IoT sensors is poor. The data is usually collected by smartphones which have an integral role in IoT. The user interface for IoT applications are provided by the smartphones. However, they are not a good option. The above fact is illustrated with the help of example below according to [15]:

Consider the example of home automation: in case of critical home-monitoring and security applications, is it worth to rely upon a smartphone. What will happen?

- When the person's smartphone goes into airplane mode during his travel?
- Does the electricity shut down or, his home security gets interrupted?
- What if the sensors stopped working abruptly?

V. CHALLENGES OF INTERNET OF THINGS

1. Security:

IoT has happened to cause major security issues that have grabbed the attention of various public and private sector companies of the world. Adding such a massive number of new hubs to the systems and the web will provide attackers with a larger platform to invade the system, particularly as many experience the ill effects of security holes. Indications suggested that the malware captured infinite number of IoT gadgets that are being used in basic applications like smart-home devices and closed-circuit cameras and deployed them against their own servers. A further critical move in security will develop from the way IoT turns out to be involved in our lives Some study proves that cameras connected to the internet will contribute 30% to security concerns. Others are being 15% on house doors, 12% on cars, 10% on TVs, 6% due to iron, 6% on heating systems, 6% on smoke systems, 5% and 5% on an oven and lightening each.

2. Connectivity:

The most significant challenges of the future of IoT would be to connect several devices, this communication will end up resisting the currently existing structure and the technologies associated with it. Presently, a centralized, server/client architecture is being utilized to authenticate, authorize and connect several terminals in a network [9].This model is appropriate only for the current situation and is not scalable to cater future needs where billions of devices will be part of a single network. This scenario will transform the current centralized system into a bottleneck. Large amount of investments and expenditure in maintaining the cloud clusters of servers are required which can deal with humongous quantity of information exchange, as unavailability of servers can lead to a total system shutdown.

3. Compatibility and Longevity:

IoT is developing in a widespread manner. It is incorporating many technologies and will soon advance into a convention. This will pose serious challenges and will demand setting up of additional software and hardware in order to establish communication amongst the devices. Unavailability of standardized M2M protocols, Non-unified cloud services, and varieties in firmware and operating systems among IoT devices are some of the other compatibility issues. Devices working on these technologies will become purposeless in future as these technologies are going to become outdated very soon.

4. Standards: Technology conventions incorporating network and communication protocols, and data-aggregation conventions, are the collection for activities that handle, process and store information obtained from several sensors. These enhance the data by increasing the scale, scope, and frequency of data available for analysis [9, 10].

5. Intelligent Analysis & Actions:

The final step in the implementation of IoT is the revelation about the data for analysis. The analysis procedure is based on cognitive technologies and models. There are certain parameters that cause intelligent actions to be incorporated in IOT, some of them being lesser device cost, enhanced device functionality, the machine "influencing" human actions through behavioral-science rationale, deep learning tools, machines' actions in unusual scenarios, information security and privacy and device interoperability [11].

VI. HIGH LEVEL SECURITY STANDARD

The Security Standard Concerns as the Following Fig 6.1 [14].

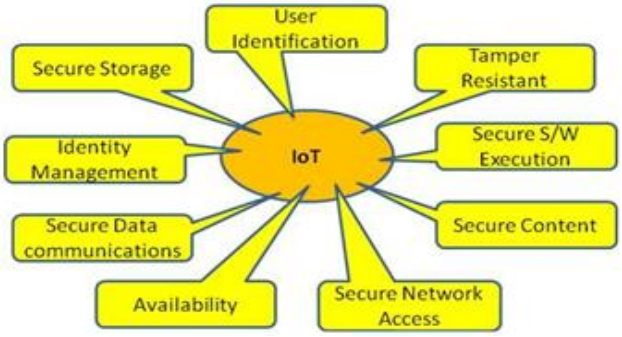

Fig.1. IoT high level Secutity Standard.

1. User identification: It refers to the process of validating users before allowing them to use the system.
2. Tamper resistance: It refers to the desire to maintain these security requirements even when the device falls into the hands of malicious parties, and can be physically or logically probed.
3. Secure execution environment: It refers to a secure, managed-code, runtime environment designed to protect against deviant applications.
4. Secure content: Content security or Digital Rights Management (DRM) protects the rights of the digital content used in the system.
5. Secure network access: This provides a network connection or service access only if the device is authorized.

6. Secure data communication: It includes authenticating communicating peers, ensuring confidentiality and integrity of communicated data, preventing repudiation of a communication transaction, and protecting the identity of communicating entities.
7. Identity Management: It is broad administrative area that deals with identifying individuals / things in a system and controlling their access to resources within that system by associating user rights and restrictions with the established identity.
8. Secure storage: This involves confidentiality and integrity of sensitive information stored in the system.

VII. CONCLUSION

Standard Security on IoT it is necessary and crucial with powefull security In indicators which will prevent and protect against harm and economical losses .In this paper focus on the importance of IoT safety and the best way to get the highest stages of safety in the light of quality standards and indicators And how to deal with challenges and help with solutions for the future.

REFERENCES

[1]. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), 1645-1660.

[2]. Li, S., Da Xu, L., & Zhao, S. (2015). The internet of things: a survey. Informtion Systems Fronties,17(2), 243-259.

[3]. IBM, "Smart China report," 2009.

[4]. N. Bari, G. Mani, and S. Berkovich, "Internet of things as a methodolog- ical concept," in Computing for Geospatial Research and Application (COM. Geo), 2013 Fourth International Conference on. IEEE, 2013, pp. 48–55.

[5]. Coetzee, L., & Eksteen, J. (2011, May). The Internet of Things-promise for the future? An introduction. In IST-Africa Conference Proceedings, 2011 (pp. 1-9). IEEE.

[6]. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December). Future internet: the internet of things architecture, possible applications and key challenges. In Frontiers of Information Technology (FIT), 2012 10th International Conference on (pp. 257-260). IEEE.

[7]. Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqa, A., & Yaqoob, I. (2017). Big IoT data analytics: Architecture, opportunities, and open research challenges. IEEE Access, 5, 5247-5261.

[8]. Desai, P., Sheth, A., & Anantharam, P. (2015, June). Semantic gateway as a service architecture for iot interoperability. In Mobile Services (MS), 2015 IEEE International Conference on(pp. 313-319). IEEE.

[9]. Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., ... & Doody, P. (2011). Internet of things strategic research roadmap. Internet of Things-Global Technological and Societal Trends, 1(2011), 9-52.

[10]. Sheng, Z., Yang, S., Yu, Y., Vasilakos, A., Mccann, J., & Leung, K. (2013). A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities. IEEE Wireless Communications, 20(6), 91-98.

[11]. Theoleyre, F., & Pang, A. C. (Eds.). (2013). Internet of Things and M2M Communications. River Publishers.

[12]. James Kirkland , "Internet of Things: insights from Red Hat" , Website:https://developers.redhat.com/blog/2015/03/31/internet-of-things-insights-from-red hat/ , Accesed :2nd February 2018.

[13]. Koivu, A., Koivunen, L., Hosseinzadeh, S., Laurén, S., Hyrynsalmi, S., Rauti, S., & Leppänen, V.(2016, December). Software Security Considerations for IoT. In Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on (pp. 392-397). IEEE.

[14]. Sachin Babar,Antonietta Stango,Neeli Prasad,Jaydip Sen,Ramjee Prasad .(2014, may). Proposed Embedded Security Framework for Internet of Things.Conference: 2nd IEEE International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE).

[15]. Banafa, A. (2014). IoT and Blockchain Convergence: Benefits and Challenges. IEEE Internet of Things.