IJFEAT

INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

INTERNET OF THINGS

Sakshi Girish Dubewar[1], Aditi Avinash Pande[2]

[1]*Student, Information Technology, Dr. N. P. Hirani Institute of polytechnic, Pusad, Yavatmal, Maharashtra, India,* ***sakshidubewar@gmail.com***

[2]*Student, Information Technology, Dr. N. P. Hirani Institute of polytechnic, Pusad, Yavatmal, Maharashtra, India,* ***aditipande011@gmail.com***

ABSTRACT

The Internet of Things is emerging as the third wave in the development of the internet. Internet of things (IoT) is expected to have a massive impact on consumer products, business and wider culture, but these are still early days. Given its potential for very wide applicability to almost all verticals and aspects of business, industries, manufacturing, consumer goods, supply chains, etc.. IOT as a whole is very broad area. This paper focuses specifically to its adoption to our Homes. Examines current leading companies in the market and technologies driving the same. Importantly based on analysis of current consumer sentiment about the new smart devices, carves out the potential opportunities to bring down the barriers the Internet of Things is facing on its way to mainstream adoption and who has potential to win in this segment.

INTRODUCTION

The internet has played a fundamental role in our lives by allowing people to connect across continents and has brought us closer as a race. The first internet wave made it possible to connect 1 billion users via personal computers in the 1900s. This was followed by the mobile internet wave which resulted in more than 2 billion additional connected users since early 2000. The next wave, which has already begun, will connect up to 50 billion "things" to the internet by 2020 up from the 10 billion which are already connected today. We are at the cusp of realizing the full potential of the information collected through these internet of things (IoTs). Up until the dawn of this decade (2010s), the devices connected to the internet have predominantly been homogenous (PCs or smartphones) and used primarily for communication purposes. The next wave of "things" ranging from the wearables such as smart watches and glasses to smart refrigerators and door locks are going to be heterogeneous. To some degree currently each smart product functions on its own but doesn't connect to other things as people in day to day expect, to create value things need to talk to other things and need to go beyond just providing remote control functionality. So, in order for a smart home containing this heterogeneous set of things to operate with little or no human intervention a management system will be needed.

MARKET TRENDS

The Internet of Things is a phenomenon where tiny machines have the ability to sense, respond, compute, and connect to the Internet, providing unprecedented access to control things and the environment around us. While it is still in its infancy, the time is ripe now with all the key ingredients in place – low price points for the devices, explosion of smart phones, tablets, PCs which are essential for providing the ability to manage and control the devices, broadband access to the Internet in homes, consumer demand, and manufacturers providing the capabilities to differentiate their products for an explosive growth over the next decade. Home automation with the proliferation of IoT is becoming a reality now, and a variety of players like, Apple, Amazon, Google, Samsung, are all converging into this space to provide the platform and solutions for smart homes. Homes account for more than 30% of electricity usage, have natural overlap with consumer oriented devices (e.g., smart phones), and ample room to digitize. While the concept of "smart homes" has existed since the 1960s, the house remains one of the few elements in our lives still governed by physical / analog solutions. Digitization within the home is going to increase, specifically in home energy efficiency, home comfort, and security as initial key areas of focus. Connected - home device shipments will grow at a compound annual rate of 67% over the next five years, much faster than smart phone or tablet device growth, and hit 1.8 billion units shipped in 2019, according to BI Intelligence estimates. Connected home devices include all smart appliances (washers, dryers, refrigerators, etc.), safety and security systems (internet connected sensors, monitors, cameras, and alarm systems), and energy efficient equipment like smart thermostats and smart lighting, healthcare for remote monitoring, diagnostics and services. Some of these areas like healthcare are in the stages of infancy, whereas, security and energy efficient equipment are in the early growth phase.

IoT Landscape

In IoT arena, current players are transformed traditional players from service sectors providing modernized Smart security/surveillance services, internet/TV/media services and Smart power utility services and new players are from emerging IOT device & gateway device manufacturers, health care related services providers and integrated management function providers. Figure 4 Diverse landscape of companies providing security solutions ADT dominates $13B Home security and automation providers market by taking around 25% or market with $3.3B revenues in 2013 with seven million customers. The ADT Corporation (ADT) is a leading provider of electronic security, interactive home and business automation and monitoring services for residences and small businesses in the United States and Canada. ADT's broad and pioneering set of products and services, including ADT Pulse® interactive home and business solutions, and health services, meet a range of customer needs for today's active and increasingly mobile lifestyles

CURRENT BARRIER

Many studies show that the adoption of IOT devices at home are going to be quite high in mid to long term, main barrier for a faster growth is that 'not many people heard of Internet of things'. Among those aware of these devices are concerned about the perceived value of these devices, price, fear of new technologies, security and privacy . Consumers are more willing to pay higher prices for safety devices like smart alarms and smart smoke detectors. Better consumer education about benefits of these devices will help in early adoption of these devices by many households. Consumers are also willing to purchase smart devices like smart thermostats if these are offered instead of standard devices in the stores.

REGULATIONS

The Federal Trade Commission is examining the emerging role of connected technology and the ramifications for user privacy and data security. FTC recently handed down 20year Consent Order 25 to TREND net over the company's "secure" webcams which were due to faulty software. FTC is taking a serious look at what kind of regulatory steps or oversight are necessary for personal and home devices that collect unique user data and transmit it over the Internet. 26 FDA also has developed guidance document to assist industry and FDA staff in identifying and appropriately addressing specific considerations related to the incorporation and integration of radio frequency (RF) wireless technology in medical devices. This guidance highlights and discusses RF wireless technology considerations that can have an effect on the safe and effective use of medical devices. These considerations include the selection of wireless technology, quality of service, coexistence, security, and electromagnetic compatibility (EMC). Consideration of these areas can help provide reasonable assurance of safety and effectiveness for medical devices that incorporate RF wireless technology, and are supplementary to other device specific guidelines. 27 4.2.

SOCIETAL IMPACT

Societal impact of auto data collection by sheer number of IoT devices, likely in 100s of billions, is huge as this data could be used in ways that change how humans and devices, humans and humans, and, data owners and service providers interact. Medical data collected by medical IoT devices help patients remotely treated by doctors transforming the current model of visiting doctors office or hospital for any kind of illness. Smart power devices may help control the power consumption to an extent that makes local governments & power utility companies self sufficient in energy that lessen the need to search for alternate and more greener energies. Increased privacy concerns that arise out of huge data management and data usage likely to increase governmental regulations in the wireless communications and user data access. Societal impact is hard to predict as it is hard to predict the adoption of variety of IoT devices.

COMMUNICATION

Zigbee or Thread like suite of high level communication protocols to create personal area networks, designed specifically for the home. Mesh network designed to securely and reliably connect hundreds of products around the home – without blowing through battery life. Designed to support a wide variety of products for the home: appliances, access control, climate control, energy management, lighting, safety, and security. Designed to have extremely low power consumption. Devices efficiently will communicate to deliver a great user experience; yet will run for years on the smallest of batteries.

Embedded OS for IoT devices

Software designed to require as little battery power and memory as possible. It is based on a microkernel and designed for energy efficiency, hardware independent development, a high degree of modularity. Supporting 6LoWPAN, IPv6, RPL, TCP, and UDP.

SECURITY

While security considerations are not new in the context of information technology, the attributes of many IoT implementations present new and unique security challenges. Addressing these challenges and ensuring security in IoT products and services must be a fundamental priority. Users need to trust that IoT devices and related data services are secure from vulnerabilities, especially as this technology become more pervasive and integrated into our daily lives. Poorly secured IoT devices and services can serve as potential entry points

for cyber attack and expose user data to theft by leaving data streams inadequately protected.

The interconnected nature of IoT devices means that every poorly secured device that is connected online potentially affects the security and resilience of the Internet globally. This challenge is amplified by other considerations like the mass-scale deployment of homogenous IoT devices, the ability of some devices to automatically connect to other devices, and the likelihood of fielding these devices in unsecure environments.

As a matter of principle, developers and users of IoT devices and systems have a collective obligation to ensure they do not expose users and the Internet itself to potential harm. Accordingly, a collaborative approach to security will be needed to develop effective and appropriate solutions to IoT security challenges that are well suited to the scale and complexity of the issues.

ADVANTAGES

Here are some advantages of IoT:

1. **Data**: The more the information, the easier it is to make the right decision. Knowing what to get from the grocery while you are out, without having to check on your own, not only saves time but is convenient as well.
2. **Tracking**: The computers keep a track both on the quality and the viability of things at home. Knowing the expiration date of products before one consumes them improves safety and quality of life. Also, you will never run out of anything when you need it at the last moment.
3. **Time**: The amount of time saved in monitoring and the number of trips done otherwise would be tremendous.
4. **Money**: The financial aspect is the best advantage. This technology could replace humans who are in charge of monitoring and maintaining supplies.

Disadvantages

Here are some disadvantages of IoT:

1. **Compatibility**: As of now, there is no standard for tagging and monitoring with sensors. A uniform concept like the USB or Bluetooth is required which should not be that difficult to do.
2. **Complexity**: There are several opportunities for failure with complex systems. For example, both you and your spouse may receive messages that the milk is over and both of you may end up buying the same. That leaves you with double the quantity required. Or there is a software bug causing the printer to order ink multiple times when it requires a single cartridge.
3. **Privacy/Security**: Privacy is a big issue with IoT. All the data must be encrypted so that data about your financial status or how much milk you consume isn't common knowledge at the work place or with your friends.
4. **Safety**: There is a chance that the software can be hacked and your personal information misused. The possibilities are endless. Your prescription being changed or your account details being hacked could put you at risk. Hence, all the safety risks become the consumer's responsibility.

APPLICATION

- Smart home
- Connected car
- Industrial internet
- Smart cities
- IoT in agriculture

CONCLUSION

Although IoT has quite a few disadvantages, its advantages of saving the consumer time and money can't be ignored. So the time isn't far when the Internet Of Things will be commonly seen in both households and companies. Efforts will have to be made to find ways to combat its disadvantages.

REFERENCES

[1] K. Ashton, That ―Internet of Things‖ Thing, RFID Journal. (2009).
[2] H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realising the Internet of Things, Cluster of European Research Projects on the Internet of Things - CERP IoT, 2010.
[3] J. Buckley, ed., The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems, Auerbach Publications, New York, 2006.