Digital Transformation- The Internet of Things- Opportunities and Challenges

Rachana C R,
Associate Professor & Head, DoS in Computer Science,
PG Wing of SBRR Mahajana First Grade College (Autonomous)
Pooja Bhagavat Memorial Mahajana Education Centre,
K.R.S. Road, Metagalli, Mysuru-16.

ABSTRACT

Internet of Everything is the most promising domain in the world of Connectivity which encompasses the Internet of Things. The Internet of Things refers to assigning digital identifiers to objects around us, allowing inanimate things like devices, electronic appliances, vehicles, and others to be remotely accessed by human for ease of use and convenience. The Internet of Everything brings together people, process, information and objects to make networks of Communication more meaningful and valuable than ever before, thus providing economic opportunities for businesses and individuals. IoE will help businesses achieve this goal by creating newer opportunities for greater optimization and efficiencies. The Internet of Things has taken over the business markets over the last few years. The viable benefits of IoE has encouraged and empowered Entrepreneurs through cost-cutting, efficient execution of innovative business ideas. People experience the environment around them through their senses (hearing, touch, sight, taste, and smell). In this context, IoE is an exponential proxy for sensing, understanding, and managing the world around. This paper focuses on exploring the huge competitive advantages for organizations who adopt IoT/IoE based technologies. Further, the paper also discusses the important challenges of Information Technology, specific to the Internet of Everything.

Keywords: *Business, Botnet, Challenges, IoE, IoT, Security.*

I. INTRODUCTION

IoT is the most promising technology anyone could have heard of! IoT is a system that interconnects various computing devices in a single network. Smart cities, Smart homes, Connected cars, Smart Logistics, Smart Agriculture, Smart utilities, and Wearable gadgets are the result of Internet of Everything. Ted Hebert at Globalsign notes that, “In 2019 Amazon reported 100 million Alexa smart devices had been sold. It took thirteen years for televisions to reach the 50 million mark in the U.S. alone, versus two for smart speakers. It took four years for internet access to reach 50 million, and two years for Facebook”. The numbers depict the alarming pace at which information is disseminated and communicated across the globe with the amazing technology- IoE. The IoE market is driven by rising adoption of Machine to Machine technology and rise in cloud-based services. The advent of disruptive technologies such as IoT, Big Data, Robotics and others are also creating a favourable environment for the growth of the IoE market.

IoE- The Internet of Everything is the final evolutionary stage of the connected world. Previously unconnected, physical-first objects and processes, as well as humans, converge to the point of connectivity i,.e the connected world. IoT- The Internet of Things is connecting the physical-first domain, which does not generate digital data unless augmented or manipulated. IoD- The Internet of Digital is the digital-first domain—that is, the “traditional” Internet, where digital data points are readily available. IoH- The Internet of Humans refers to interactions between humans and the IoT and IoD. This can involve both direct user input (e.g. by controlling a digitally connected product) or indirect human monitoring (e.g. by using wearable and a Quantified Self application).

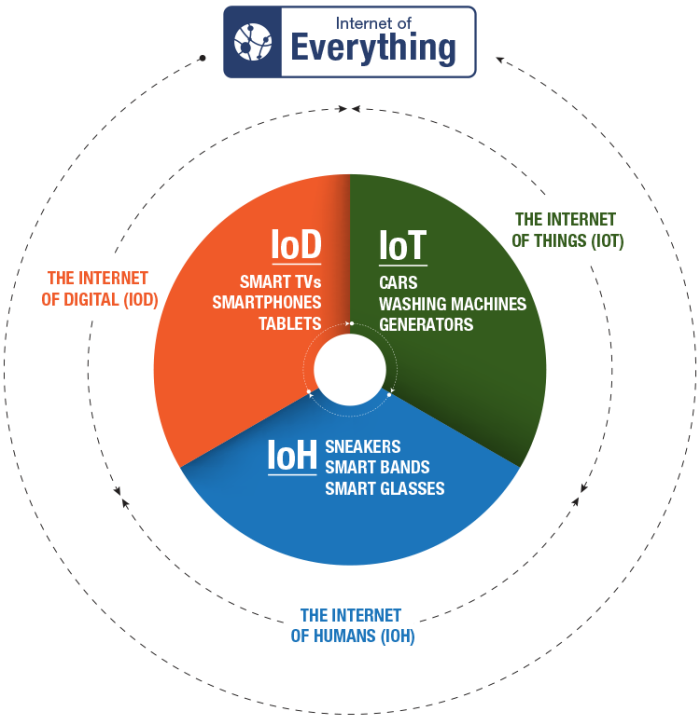

Fig 1 : The Internet of Everything

IoE Constituent Elements:

The Key components of the IoE market are hardware, software and services. The constituent elements of the Internet of Everything are:

People: People provide their personal data via websites, applications or connected devices they use such as social networks, healthcare sensors and fitness trackers etc; Artificial Intelligence algorithms and other smart technologies analyze this data to "understand" human issues and deliver relevant content according to their personal or business needs which helps them quickly solve issues or make decisions.

Things: Smart objects embedded with sensors and actuators generate data and this is sent to the destination across the network.

Data: Rather than simple collection of data, the connected devices will be sending processed data to the respective servers for evaluation or for more intelligent decision making. Data is summarized, classified and analyzed. The resulting output turns into priceless information that can control various systems and empower intelligent solutions.

Process: Different processes based on Artificial Intelligence, Machine Learning, social networks or other technologies ensure that the right information is sent to the right person at the right time.

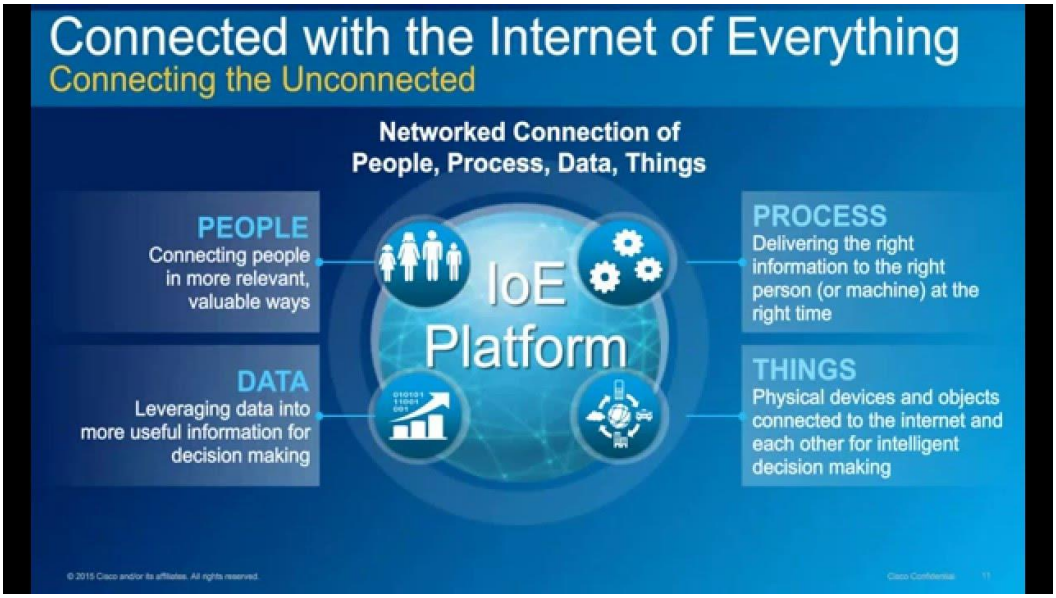

Fig. 2: Constituent elements of IoE

II. IoT/E: Advantages

A few significant examples of IoE include:

- A smart thermostat that intelligently adjusts the temperature.
- Door locks that can be controlled wirelessly over a Bluetooth connection.
- Smart light bulbs that can be controlled with a smartphone app, a wristband to pay for groceries with the help of the owner's heartbeat.
- Stores that will monitor your eye gaze, keeping track of which product you gazed at, what you picked up and thought of purchasing, but put it back on the shelf, and finally Dynamic pricing will entice you to pick it up again.
- Self-driving cars with IoE that will make traffic congestions an obsolete issue.
- Wearable devices that will be monitoring one's health statistics and the related reports will be continuously monitored by the patient himself/herself. Moreover, Sensor-based technology in jewellery, or even micro-devices embedded under the skin or inside the body will prove worthwhile in many applications relating to human body.
- With sensors on trees, the wireless system that will be helping the officials and staff to track forest growth rates in real time, in order to estimate if they are developing well and detect early infections or pest attacks.

In a smart factory, IoT has proved to lead to better inventory management, improved production processes and faster delivery times. Sensors on the factory floor are constantly transmitting data at every step of the manufacturing process to provide operators with information they need to produce. This results in assured productivity and ensures on-time delivery. The IoT enabled business intelligence system can even enable a company to proactively send a technician to fix a machine before it breaks down.

As pointed out by Bertil Thorvaldson, ABB Robotics, "The power of the Internet of Things comes from the ability to collect a lot of data and convert that into useful information". The Industrial Internet of Things (IIOT) involves the use of IoT technologies in manufacturing processes and across supply chains. Alongside data from devices and sensors, Industrial IoT strategies incorporate machine learning and big data technology. The combination of existing sensor data, machine to machine communication and automation technologies will provide more insight back to the business.

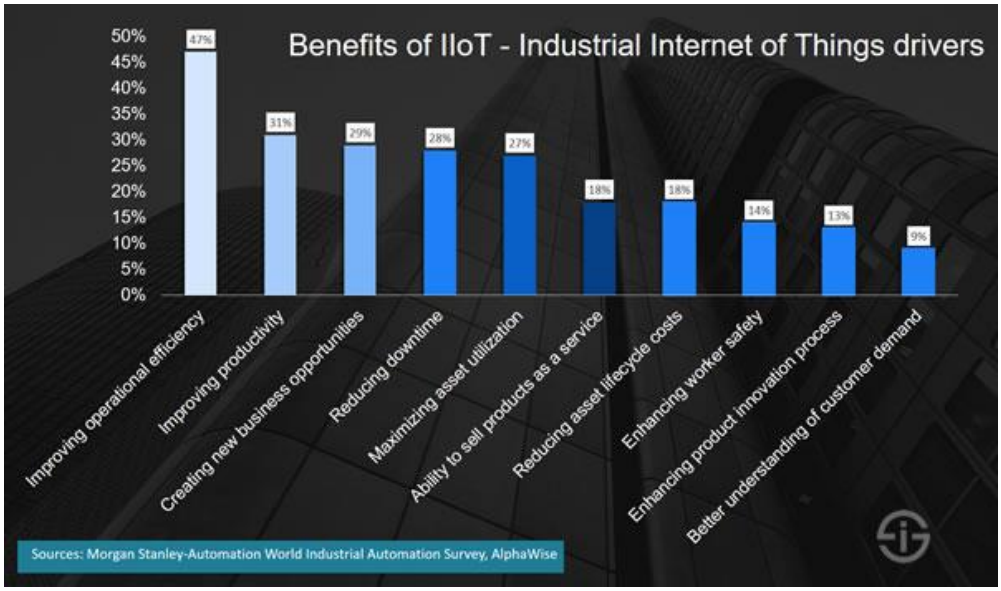

Fig. 3: Benefits of Industrial IoT – the Industrial Internet of Things drivers

III. CHALLENGES:

Technology is indeed affecting privacy of individuals in innumerable ways. Each day, one can witness the outcome of how big data is mining information of consumers for gain. Connectivity without barriers brings in huge Information Technology challenges.

Few security challenges which intrude the ethical functioning of IoE include Managed/Unmanaged Desktops, Spam/Malware, DDoS, Compromised Hosts - Remotely Controlled, Rapidly Changing Environment and so on. There are a number of instances of security breach in the working of IoE. Home/industrial/commercial appliances are tested, measured and certified for traditional qualities (e.g., durability, fit-for-purpose, maintenance, etc.).Similarly, appliances should be subjected to rigorous cyber security testing to the same degrees. But, standardized and independent verification of IoE devices, in terms of security, is still in its nascent stage. IoE is driven by an ecosystem which consists of many layers and protocols, and each of these layers can be exploited due to its vulnerability features. There are significant hardware/software vulnerabilities which endanger the IoE ecosystem. It could be a sniffer attack, where a program called ‘sniffer’ sniffs out any unencrypted information which is being passed through a network, or a compromised key attack, where the key to encrypted data is stolen and is then used to interpret the encrypted data, or an attack where cybercriminals break into a network or a device by guessing or stealing the password.

One of the most important challenges for IoE is a Botnet. Botnet is a combination of two words ‘Bot’ and ‘Net’. Bot is a word formed from ‘robot’. It is a computer which is infected by malicious software. ‘Net’ is the word formed from ‘network’, a group of systems that are linked together. A botnet is nothing but a network of infected computers, where the network is used by the malware to spread malicious information across computers/hack into systems. In 2016, the Mirai botnet, a malware written by three programmers, Paras Jha, Dalton Norman, and Josiah White shut down a large portion of the internet, including Twitter, Netflix, CNN and other major sites, as well as major Russian banks and the entire country of Liberia. The malware was discovered in 2016 by a malware research group called MalwareMustDie. This botnet is a DDoS (denial-of-service) attack which took advantage of unsecured Internet of Things (IoT) devices. It closed down a pivotal U.S. dynamic host service providing company which triggered a widespread internet outage in the USA and Europe.

The most significant threat is the exposure of the databases of biometric. Once biometric data is compromised, there is no way to rectify it. One can update the password but not the fingerprint! The challenges are innumerable.

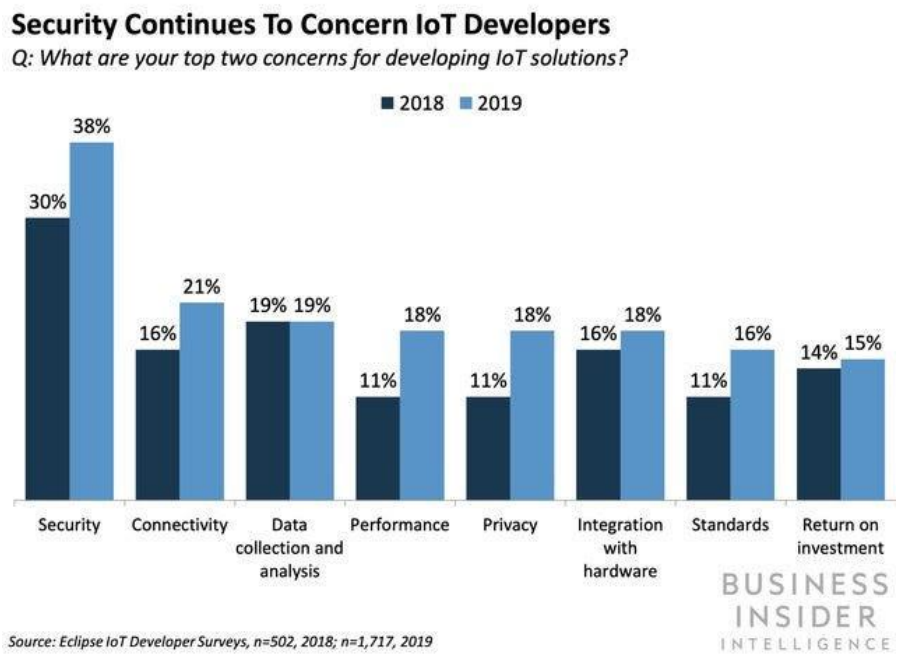

Fig.4: Security concerns of IoT developers.

With all of the benefits of Smart Devices and applications of IoT comes- Risk. With the increase in connected devices, hackers and cyber criminals gain exposure to many more entry points. Manufacturers are often presented with economic and technical challenges while building and maintaining robust security features in IoT devices. But devices and services with weak security are vulnerable to cyber attacks and can expose user data to malicious activities. An increasing number of IoT devices increases the number of potential security vulnerabilities. Ensuring security in IoT products and services must be the most important priority for vendors. Users need to trust that IoT devices and related data services are secure, especially because they are all pervasive and integrated into their daily lives.

IV. CONCLUSION

The Internet of Things applications are growing rapidly in all the stages of life. Today's networks are already loaded with the popularity of real-time applications such as e-commerce, video conferencing, online collaboration tools, video streaming services, and real time file sharing. The demand for bandwidth to accommodate IoT based services is exploding. Smart objects, wearable devices—that fall under the IoE umbrella are here to stay. Advancements in technology will spread wide enough, with multiple manufacturers, platforms, and software to choose from in the years to come. It will be quite challenging for everyone to ensure that their data is safe while using IoE-enabled devices. Furthermore, the challenges experienced with IoT can definitely be overcome as companies adopt IoT to enjoy the full benefits. In the current trend toward digitalization, manufacturers increasingly rely on a wide range of technology platforms to help streamline and accelerate their production processes. To better understand and utilize Industrial Internet of Things (IIoT) data, organizations are deploying multiple, single-use systems and tools, such as Artificial Intelligence (AI), data analytics, or Virtual Reality (VR). The issue which concerns is that the vendors sell these technologies individually and since they lack integration, companies are unable to capitalize on the information they've gathered. After deployment, the business and IT leaders are able to realize the value and effectiveness of the unified platform.

REFERENCES:

[1] Stephen Cobb, Botnet malware: What it is and how to fight it, welivesecurity, October 2014.
[2] Top 12 Benefits of Chatbots: Comprehensive Guide [2020 update], Drift's 2018 State of Chatbots Report, January 1, 2020.
[3] Ehtesham Peerzade, IoE Market Size, Business Opportunities, Growth, Segments, Industry Profits and Trends by Forecast to 2023, Feb 28 2020.
https://www.tradove.com/blog/IoE-Market-Size-Business-Opportunities-Growth-Segments-Industry-Profits-and-Trends-by-Forecast-to-2023.html

[4] https://ioe.org/
[5] IoT Resource Web page, http://www.internetsociety.org/iot.
[6] The Internet of Things (IoT): An Overview - Understanding the Issues and Challenges of a More Connected World. (2015).
[7] https://www.businessinsider.com/iot-security-privacy?IR=T
[8] https://knowledge.wharton.upenn.edu/article/leveraging-the-internet-of-things-for-competitive-advantage/
[9] https://www.weblineglobal.com/blog/how-enterprises-can-take-the-advantage-of-iot/
[10] https://www.iot-now.com/2019/05/10/95621-iot-opportunity-network-competitive-advantage/
[11] https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-iiot-saving-costs-innovation/
[12] https://www.information-age.com/advantages-industrial-iot-secure-123470377/
[13] https://www.iotworldtoday.com/2020/04/17/gartner-magic-quadrant-for-industrial-internet-of-things-2019/
[14] https://www.abiresearch.com/pages/what-is-internet-things/
[15] https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/explaining-all-things-ioe