National Conference on Recent Advances in Computer Science and IT (NCRACIT)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 1 | ISSN : 2456-3307

Bringing AI to the IoT- Developing an INTELLIGENT IoT (IIoT)

Muneer Ahmad Dar[1], Tahir Mohammad wani[2], Sahil Nazir Pottoo[3], Sameer Ahmad Mir[4]

[1,2,3,4]Department of ECE, SoET, Baba Gulam Shah Badshah University, Rajouri, J&K, India
darmuneer1@gmail.com[1], tahir086991@gmail.com[2], Sahilpottoo294@gmail.com[3], ersameerece@gmail.com[4]

ABSTRACT

This paper provides an overview of the recent developments in the IoT technology and the challenges that IoT is facing now or going to face in the near future. This paper also predicts how AI as a technology can be used in combination with IoT to overcome these challenges. In our study, we took some practical examples of IoT to understand how it is reshaping our daily lives and tried to evaluate the need and impact of merging AI with it.

Keywords: IoT, Artificial Intelligence, Big Data, Smart Objects

I. INTRODUCTION

The increasing number of physical objects are being connected to the Internet at an unprecedented rate realizing the idea of the Internet of Things (IoT). A recent report states that "IoT smart objects are expected to reach 212 billion entities deployed globally by the end of 2020".[1] IoT creates a tremendous amount of data. That data can be captured (enter: big data) and analyzed. It is not realistic to do this tracking by human effort, given the sheer volume of data. But, one of the IoT's greatest attributes is its ability to integrate and work with other emerging technologies. AI, artificial technology, can serve an important role in tracking, going through this mountain of IoT data and distilling it into actionable themes.

Our world is facing a rapid expansion of devices and sensors that are connected to the Internet. So many new nodes being added to networks and the internet will provide malicious actors with innumerable attack vectors and possibilities to carry out their evil deeds, especially since a considerable number of them suffer from security holes. From the fact that IoT will become more ingrained in our lives. Our very lives and health can become the target of IoT hack attacks. Creating systems that can adequately secure equipment from intentional and accidental malicious use is challenging. AI may be used to develop context-aware security systems and alarms for IoT devices. The sheer volume of data that gets created by the newly connected IoT devices is increasing constantly. This data holds great value as it helps in deriving useful insight into what's working well or what's not. The problem arises while finding out ways to analyze massive amounts of performance data and information coming from these devices. It is simply impossible for humans to understand and review terabytes of data. Thus, AI, artificial technology, which is a much more subject of interest nowadays, can prove a useful tool while dealing with the problems of such kind in the IoT based systems. In the recent practical studies it has been found that the AI has already out-smarten the human beings while solving the real world problems

with much more accuracy and in least time.[2] Thus for improving the speed and accuracy of analyzing data coming through sensors enabled devices, AI in IoT is to be used. MIT proposes taking IoT to its next natural cognitive level. This means adding some AI across the entire IoT network to make it self-aware. [3]

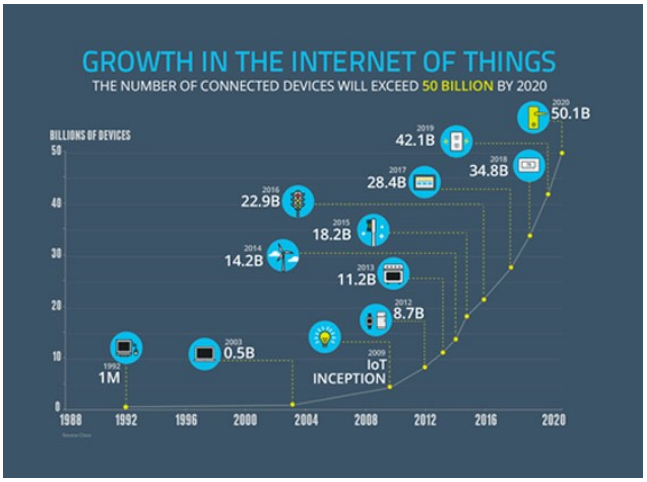

Figure 1. Exponential Growth in the IoT

Furthermore, companies are finding that machine learning, an AI technology, can have significant advantages over traditional business intelligence tools for analyzing IoT data, including being able to make operational predictions up to 20 times earlier and with greater accuracy than threshold-based monitoring systems. In this paper [4], we made a study of the problems that IoT is facing now or going to face in the near future and how the AI as a tool can be used to deal with them.

II. INTERNET OF THINGS

In 1999 a British pioneer named Kevin Ashton describe the IOT as a system where objects in the physical world could be connected to the internet by sensors.[5] Things mean everything's and anything's like goods, objects, machines, appliances, vehicles and even ourselves will become a part of this internet of things. To turn things into smart things in the internet of things .firstly we have to give them unique identity (IPv6 give us this unique identity), secondly we need to give them the ability to communicate, and in addition to that we need to add sensor.

III. ARTIFICIAL INTELLIGENCE

Artificial Intelligence is a suite of technologies capable of affording machines perception and cognition. Perception allows digital systems to observe themselves and the surrounding world through sensors and other data streams. Cognition allows machines to learn rules and to solve problems based on examples and models. These elements combine such that machines may develop an almost human-like intuition, with an awareness of their own place, purpose, and processes

IV. CHALLENGES IN HARNESSING THE FULL POTENTIAL OF IOT AND NEED FOR AI

The Internet is a powerful tool used in all kinds of the information systems. The network is available almost anywhere, at home, at work, also on mobile devices (phones, watches). People start to think to connect the Internet to almost all devices of everyday use, so they can communicate with each other by taking simple decisions for people and helping them in their life. Such idea is called the Internet of Things (IoT). It is estimated that currently about 15 billion devices are connected to the Internet, but this number is still less than 1% of things that in fact could be connected to the network.[6] As the number of connected devices will increase so will be the challenges for a future IoT network.

Here we listed the three most important challenges that IoT technology is going face and how the AI will help in overcoming them:

a) Security

IoT has already turned into a serious security concern that has drawn the attention of prominent tech firms and government agencies across the world. The hacking of baby monitors, smart fridges, thermostats, drug infusion pumps, cameras and even the radio in your car are signifying a security nightmare being

caused by the future of IoT. So many new nodes being added to networks and the internet will provide malicious actors with innumerable attack vectors and possibilities to carry out their evil deeds, especially since a considerable number of them suffer from security holes.

The more important shift in security will come from the fact that IoT will become more ingrained in our lives. Concerns will no longer be limited to the protection of sensitive information and assets. Our very lives and health can become the target of IoT hack attacks. Creating systems that can adequately secure equipment from intentional and accidental malicious use is challenging. AI may be used to develop context-aware security systems and alarms for IoT devices.

This AI leverages the fact that most IoT devices are mirrored in the Cloud or another central repository with scalable computing. Physical system behavior is observed, with sparse data being sent to a digital duplicate using a model to "interpolate" these data into a rich representation. This model starts out as generalized by object type, but over time adapts to the particular nuances of the mirrored object's own sensors, environment, and use cases. These models interact with one another in the Cloud so that they learn their place in a larger system. "Cognitive Firewalls" and "Cognitive Supervisors" use each model to evaluate the impact of commands to ensure they are benign prior to execution, or to identify when a process behaves anomalously. The Firewall uses the adaptively learned model to "test" a command digitally to ensure it does not violate any known or learned limits prior to forwarding it to the related physical device. For example, the Cognitive Firewall could be used to protect a robot arm from malicious commands. When the arm is sent commands that cause the arm's mirror to intersect with a second robotic arm in the same Cloud Factory, the command is rejected.[5] Thus, AI can teach devices and services right from wrong, not to believe everything they hear, not to take advice from strangers, and cause the effect. These examples show the potential for Artificial Intelligence to supervise and protect digitally mirrored systems. AI will also be able to help better secure the IoT world by anticipating and fighting intruders more quickly than human beings can.

B) Analyzing Big Data

"IoT smart objects are expected to reach 212 billion entities deployed globally by the end of 2020".[1] Our world is facing a rapid expansion of devices and sensors that are connected to the Internet. The sheer volume of data that gets created by them is increasing constantly. IoT will produce a treasure trove of big data – data that can help cities predict accidents and crimes, give doctors real-time insight into information from pacemakers or biochips, enable optimized productivity across industries through predictive maintenance on equipment and machinery, create truly smart homes with connected appliances and provide critical communication between self-driving cars. The possibilities that IoT brings to the table are endless. The problem arises while finding out ways to analyze massive amounts of performance data and information coming from these devices. It is simply impossible for humans to understand and review terabytes of data. Machine learning, an AI technology, brings the ability to automatically identify patterns and detect anomalies in the data that smart sensors and devices generate—information such as temperature, pressure, humidity, air quality, vibration, and sound. Companies are finding that machine learning can have significant advantages over traditional business intelligence tools for analyzing IoT data, including being able to make operational predictions up to 20 times earlier and with greater accuracy than threshold-based monitoring systems.[2] To correctly process raw sensory data and make smart decisions, Internet of Things platforms require artificial intelligence.

c) The Latency

One of the major bottlenecks in connecting and controlling the devices remotely is the latency itself. Up until now, the Internet of Things (IoT) has

consisted of sensors and devices shipping data to some centralized or semi-centralized environment for processing. With fog computing, there are efforts to introduce processing and analytics power close to, or within, the devices themselves, thereby reducing latency. To understand how IoT can be a more useful and a life-saving tool with the merge of AI, let us take an example:

With the widespread adoption of wearable sensors, means that doctors and nurses can provide better health care than ever before. As our wearable has become ever more sophisticated, instead of just reading your heart rate and pace when you run, they will be able to send an alert to your doctor if they detect that you might be having a heart attack. Therefore, IoT is a good start. An AI control layer could take this to the next level. Imagine technology that receives that alert, then finds and routes the closest ambulance to you while notifying the hospital and your doctor. It then starts and drives your doctor's autonomous car (an IoT device itself), delivering him or her to the hospital as quickly as possible. So adding AI to IoT could save the critical minutes to keep you alive.

V. CONCLUSION

Augmented intelligence (AI) is helping to usher growth and prosperity in every industry across the globe. This intelligent technology is developed and used to "augment" performance and improve outcomes, but does not replace human power. Its man and machine, not operate versus machine – an important distinction when it comes to applying AI to IoT. The convergence of AI and IoT means that these physical devices can now see, hear and understand the world around them. They can make sense of the vast amount of unstructured data that is being produced and then provide businesses with more intelligent insights that enable more innovative uses, which will directly benefit all of us - both professionally at work, and personally at home. AI and IoT can provide some amazing benefits to people and the world if we use them sagely.

VI.REFERENCES

[1] Ubiquitous Computing and Ambient Intelligence: 11th International Conference.

[2] Science Magazine http://www.sciencemag.org/news/2017/04/self-taught-artificial-intelligence-beats-doctors-predicting-heart-attacks

[3] Sanjay Sarma, and Joshua E. Siegel IIC Journal of Innovation, MIT

[4] Ashton was working on RFID (radio-frequency identification) devices, and the close association of RFID and other sensor networks with the development of the IoT concept is reflected in the name of the RFID device company that Ashton joined later in his career: "Thing Magic."

[5] Dr. lng. Alexandru radovici "introduction to the internet of things"

[6] Constellation Research 2017 Digital Transformation Study

[7] http://images.huffingtonpost.com/2016-07-12-1468314021-5633148-internetofthings.jpg