# Collaborative approach of AI in Internet of Things to incorporate M2M Interaction

*Chitti T N [1], Saravanan Alagarsamy[2]*

[1]*Senior Assistant Professor, Information Science and Engineering, New Horizon College of Engineering, Bangalore, Karnataka, India.*
[2]*Associate Professor, Department of Computer Science and Engineering, Kalasalingam Academy of Research and Education, Krishnankoil, Srivilliputhur, Tamil Nadu,India*

Email: chittitn.nhce@newhorizonindia.edu

## Abstract

*AI is a branch of computer science which is a study of developing machines to perform tasks. On the other hand IoT is all about things (devices) that connect to internet to perform tasks. The primary criteria of both the techniques are to incorporate machine-machine intervention. AI provides automation to complete the tasks without any human intervention. The collaboration of both the techniques will definitely results into a better outcome. Internet of things has become very popular now. Artificial intelligence mainly uses machine learning algorithms into IoT. Artificial intelligence is used to easily identify useful patterns and anamolies form the data collected from IoT sensors. Artificial intelligence is easily embedded into various programs and chips which are all connected to IoT networks. IoT is helping the business world to capture large amount of data from various sources. In general both the techniques are very powerful where IoT (nerve), AI (brain). Artificial intelligence along with Internet of Things provides a wide range of advantages for businesses and consumers, including proactive intervention, tailored experiences, and intelligent automation. Artificial intelligence is combined with IoT which explains how the data is analyzed and makes decision and acts on the data without any human intervention. The combination of both the technologies plays a vital role in all real-time applications.*

*The combination of AI (Artificial Intelligence) with the IoT has the potential to design and develop industries, businesses, and economies to operate properly. IoT with AI generates good results that help in proper decision-making with little or no human intervention. The combination of both the technologies can help both the normal and the business people. IoT deals with devices connecting with each other over the internet and Artificial Intelligence is focused with devices learning from their data and experience.*

***Prerequisites:*** *IoT in automatic irrigation, IoT in automatic car, IoT in automatic liquid monitoring.*

# 1. Introduction

Internet of things (IoT) mainly deals with sensors and actuators. It has been proved that more than 50 billion sensors are connected to the internet now and all these sensors were helpful in sensing the data. (Radanliev et al.) These devices were mainly useful for collecting and exchanging of data. IoT devices deal with a lot of data that needs to be collected to monitor results. Internet of Things is used to collect, handle the large amount of data useful for AI algorithms. (Wang and Qiao) This algorithm converts the data in useful format suitable for IoT applications.
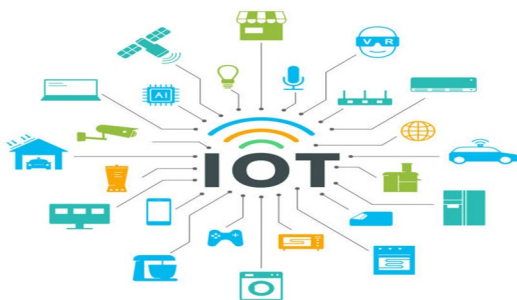


**FIGURE 1. Artificial Intelligence**



**FIGURE 2. Internet of Things**

On the other hand Artificial Intelligence (AI) is a field of study that combines computer science and robust data to achieve problem-solving. It mainly deals with building machines to perform all the tasks without any human intervention. (Melamed) It develops software that can think wisely like humans. In simple terms AI is a study of replacement of human with machine where it can perform all the tasks without any intervention. The collaboration of these technologies can be definitely useful for all sectors of people. (Comiter) It can also yields to better outcomes compared to current system. AI with artificial intelligence provides a wide range of advantages in the real – world. Some of the most common benefits of AIoT are:

## 1.1. Improves scalability:

Before sending any data from one device to another, an AIOT system analyses it and summaries the data. As a result, it can compress large amounts of data to a manageable size and allows a large number of IoT devices to be connected. This is referred to as scalability.

## 1.2. Improves customer satisfaction:

Customer satisfaction is the main priority of any business. Companies like Amazon.com, flipkart or any other online shopping cart have earned the reputation of being one of the most customer-centric businesses by prioritizing their customers' needs. All the sectors are recognizing the value of AI by using chat bots to interact with customers. (Moisejevs)

## 1.3. Predicting the result:

Many of the machine learning algorithms used in Artificial intelligence can be useful in predicting the result or outcome of any business either it can be related to profit or loss.AI in IoT can be able to predict any failures in the sensors and also helps in maintaining them.

# 2. Improves accuracy:

IoT has an ability to break large amount of data into smaller portions using many machine learning algorithms and software's that helps in minimizing the error rates and maximizing the accuracy. (Roopak, Tian, and Chambers)

# 3. Existing method

In the existing system AIoT is widely used in many real-world applications. Some of them were discussed here:

## 3.1. Robots in Manufacturing:

Robots are used in industries for mafacturing of goods instead of humans. As they were equipped with many sensors they have become smarter and they can learn the data through artificial intelligence. It will save time and money and also provides more accuracy. (Lakhani)

## 3.2. Automatic vehicles:

Self driving cars are the best examples for IoT and AI.As they are using so many IoT sensors and equipped with AI it can track the condition of the vehicle, road condition, and speed, whether and also
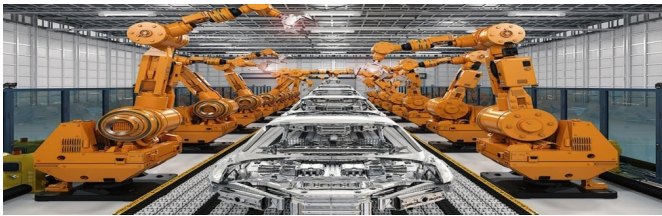
**FIGURE 3. Robots in manufacturing**

identifies the people on road which is very safe and good for every journey. (Lu and Xu)



**FIGURE 4. Tesla Autonomous car**

## 4. IoT Challenges

**Some of the technical challenges and issues that IoT is still facing are:**

### 4.1. Security:

IoT sensors and the networks connected IoT can be easily attacked by hackers which can be harmful yet not safe for the data that we are sharing.

### 4.2. Trust:

Because of the lack of security still many people are hesitant to migrate into the smarter life. A simple example can be a IoT enabled home where there is a chance of attacking by a intruder.

### 4.3. Connectivity:

Even though we are heading towards a smarter life still many villages and remote places don't have proper internet connectivity. IoT sensors enabling globally may not be easy as there is still lack of internet connection. (Rouse)

### 4.4. Energy:

As almost all the IoT sensors or devices runs using power it can be possible to charge billions of devices with the available energy. The devices or the sensors can have the short span of life and they can be totally waste later on and it can be thrown out that can lead to environmental pollution or hazard. (Mode, Calyam, and Hoque)

### 4.5. Scalability:

As IoT can convert large data into small or small data into large by incorporating various machine learning algorithms maintaining the structure of the model is one of the major challenges of IoT.

## 5. Future work

In the existing system we have discussed those basic applications of AIoT and the challenges that IoT is facing now.

To overcome some of the challenges we have proposed a technique called IoT security integrated with AI in future as security is one of the major drawbacks of IoT& AI. IoT security mainly deals with protecting IoT sensors from intruders. The sensors that are connected to the network should be encrypted and sent to the receiver. The network which is carrying the data should be encrypted using cryptographic algorithms because they can be easily penetrated to attacks. The ssid, pwd and the API key of the network should be encrypted and the data that we are transmitting to the receiver should be hidden from the attacker. To provide security to IoT devices and the data that is going through the network traffic we have to protect the devices. Using cryptographic techniques we can protect them in order to gain trust from the people so that they can use IoT sensors in order to make their life smarter.

Similarly Artificial intelligence helps IoT to initiate proper machine-machine interactions resulting in providing more accuracy in communication between one sensor with another sensor.

## 6. Conclusion

In future everything will be going to be smart and all the devices will be connected to the internet. Along with AI all branches of the science will collaboratively work in order to achieve something big. Now almost everyone was wearing smart gadgets it can be watches, belt, glasses etc. Even people are ready to take food capsules in order to track their digestive system digitally and to check out the impact of that medicine in human body. Everyone likes to live a healthy, comfortable and smart life. If it was lead-
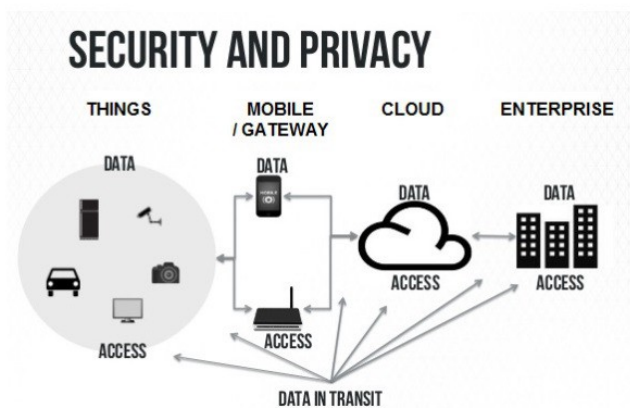
**FIGURE 5.** IoT Security

ing to constructive side it will be good otherwise it can cause destruction to mankind.

Even though it is very good to be smart but still some debate is going on regarding whether we are going towards the destruction side or not. Automation in any sector can help in improving accuracy but it doesn't need much man power that can lead to immense unemployables. Though technology is dominating our lives now still human have control over all these things where he/she can still control all the man made devices.

## References

Comiter, M. "Attacking artificial intelligence". *Belfer Center for Science and International Affairs* (2019).

Lu, Yang and Li Da Xu. "Internet of Things (IoT) Cybersecurity Research: A Review of Current Research Topics". *IEEE Internet of Things Journal* 6.2 (2019): 2103–2115.

Melamed, T. "An active man-in-the-middle attack on bluetooth smart devices". *International Journal of Safety and Security Engineering* 8.2 (2018): 200–211.

Mode, Gautam Raj, Prasad Calyam, and Khaza Anuarul Hoque. "Impact of False Data Injection Attacks on Deep Learning Enabled Predictive Analytics". *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium* (2020).

Radanliev, Petar, et al. "Artificial intelligence in cyber physical systems". *AI & SOCIETY* 36.3 (2020): 783–796.

Roopak, Monika, Gui Yun Tian, and Jonathon Chambers. "Deep Learning Models for Cyber Security in IoT Networks". *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)* (2019): 452–0457.

Wang, Shen and Zhuobiao Qiao. "Robust Pervasive Detection for Adversarial Samples of Artificial Intelligence in IoT Environments". *IEEE Access* 7 (2019): 88693–88704.

**Embargo period:** The article has no embargo period.

**To cite this Article:** , Chitti T N, and Saravanan Alagarsamy. "**Collaborative approach of AI in Internet of Things to incorporate M2M Interaction**." International Research Journal on Advanced Science Hub 05.05S May (2023): 301–304. http://dx.doi.org/10.47392/irjash.2023.S040