Intersection of Artificial Intelligence, Machine Learning, and Internet of Things – An Economic Overview

Mani Manavalan

Technology Architect, Cognizant Technology Solutions, Teaneck, New Jersey, **USA**

*Corresponding Contact:
Email: manimanavalan47@gmail.com

Manuscript Received: 05 Oct 2020 - Revised: 25 Nov 2020 - Accepted: 05 Dec 2020

ABSTRACT

Internet of Things (IoT) has become one of the mainstream advancements and a supreme domain of research for the technical as well as scientific world, and financially appealing for the business world. It supports the interconnection of different gadgets and connection of gadgets to people. IoT requires a distributed computing setup to deal with the rigorous data processing and training; and simultaneously, it requires artificial intelligence (AI) and machine learning (ML) to analyze the information stored on various cloud frameworks and make extremely quick and smart decision w.r.t to data. Moreover, the continuous developments in these three areas of IT present a strong opportunity to collect real-time data about every activity of a business. Artificial Intelligence (AI) and Machine Learning are assuming a supportive part in applications and use cases offered by Internet of Things, a shift evident in the behavior of enterprises trying to adopt this paradigm shift around the world. Small as well as large scale organizations across the globe are leveraging these applications to develop latest offers of services and products that will present new set of business opportunities and direct new developments in the technical landscape. The following transformation will also present another opportunity for various industries to run their operations and connect with their users through the power of AI, ML, and IoT combined. Moreover, there is still huge scope for those who can convert raw information into valuable business insights, and the way ahead to do as such lies in the viable data analytics. Organizations are presently looking further into the data streams to identify new and inventive approaches to elevate proficiency and effectiveness in the technical as well as business landscape. Organizations are taking on bigger, more exhaustive research approaches with the assistance of continuous progress being made in science and technology, especially in machine learning and artificial intelligence. If companies want to understand the valuable capacity of this innovation, they are required to integrate their IoT frameworks with persuasive AI and ML algorithms that allow 'smart devices/gadgets' to imitate behavioral patterns of humans and be able to take wise decisions just like humans without much of an intervention. Integrating both artificial intelligence and machine learning with IoT networks is proving to be a challenging task for the accomplishment of the present IoT-based digital ecosystems. Hence, organizations should direct the necessary course of action to identify how they will drive value from intersecting AI, ML and IoT to maintain a satisfactory position in the business in years to come. In this review, we will also discuss the progress of IoT so far and what role AI and ML can play in accomplishing new heights for businesses in future. Later the paper will discuss the opportunities and challenges faced during the implementation of this hybrid model.

Key Words: Internet of Things, Artificial Intelligence, Machine Learning, Internet of Everything

Introduction

Artificial intelligence is the skill of any mechanical gadget to mimic human intelligence. Machine Learning is an innovational subset of AI which look through information, understands it, predicts the sample, and freely develops an algorithm accordingly allowing the machines to become autonomous and program by itself. The ”Internet-of-Things (IoT)” a progressive technology that installs the internet into mechanical gadgets in a way providing them skills of recognizable proof and use of whatever type of data/results they are intended to retrieve. It additionally opens the window to cross global connection.

Moreover, AI is an innovation that is designed to make machine think and operate like humans. This ability will speed up the process of digital transformation and enable people, projects and industries all over the world. Regardless of machines, people, plants, animals, equipment, soil, stones, lakes, or literally anything a person can think of, connecting them and making ”smart decisions” will make our world an exceptional place to live and prosper together. In order to make the world and its elements really independent of each other, experts need machine learning and artificial intelligence to develop a framework that replicates human learning as well as an information analytics module in the ecosystem (Manavalan, 2018). Machine learning would create methods to handle the learning part in different components of the network to allow them to be autonomous and self-standing, while data analysis would break down each one of the data objects that are produced time-to-time for identifying the past trends and be more all the more efficient in future.

This idea has been picking up pace and technical experts are trying to integrate machine learning and data analytics into IoT sensors (Bynagari, 2018) and embedded systems (Manavalan & Donepudi, 2016) of the frameworks. The tech backing AI is truly phenomenal and this digital transformation will drive us to reevaluate all that we know about the significance of technology and make the next steps accordingly. The rate at which machine learning and data analytics are pushing artificial intelligence, calls for a need to discuss trends, challenges, and risks that will be brought by this advancement. Most probably the main idea behind this innovation is the Internet of Things that promises a world filled with intelligent devices, most of the time called ”smart objects” (Bynagari, 2019), and are internally connected via the Internet or various other communication streams.

What’s more, the Internet of Everything (Neogy & Bynagari, 2018) is likewise a comparative idea that recommends all the digital, living, and non-living things are connected via some medium of correspondence. Finally, when these ideas are formed into reality and delivered to the real world, what we get is a Cyber Physical System (CPS). In that case, a great accomplishment would be that such a world would be informatively rich so that we can accurately determine what sort of data could be useful and what sort could be dumped right away (Manavalan, 2019). This paper basically spins around ideas, challenges, and uses of artificial intelligence and machine learning in the ideas of the Internet of Things; Cyber-Physical Systems, and Internet of Everything.

Literature Review

IoT assumes a significant part in establishing a combined approach with artificial intelligence and machine learning by providing a smart framework for people (Lee and Seshia, 2016). Lately, numerous experts have presented various techniques and conventions with respect to the improvement of the quality of life with the help of machine learning and AI in IoT applications-based frameworks (Donepudi, 2018). Given below, this section presents various past works and methods which have been carried out to work on this intersection.

Bynagari & Amin (2019) proposed a method that groups and identifies the IoT gadgets in networks utilizing the supervised learning technique. The objective of this method is to give security and trustworthiness to an organization and its devices to ensure that IoT gadgets connected with other networks within the organization are secure and safely operational. It uses a supervised machine learning algorithm that identifies IoT and non-IoT gadgets in a traffic environment. In this method, a trained informational dataset of network traffics was collected, and utilizing that dataset two parameters were formed that limit the threshold and sequence size (Yang et al., 2017). Utilizing these parameters, this method recognizes IoT and non-IoT gadgets in a network traffic setting.

Donepudi (2014) proposed a deep learning-based method for dynamic IoT watermarking. This method identifies cyber attackers in a network utilizing watermarking using deep learning techniques. It utilizes long short-term memory (LSTM) algorithm based on deep learning that identifies intruders and discovers injection of data and eavesdropping in IoT gadgets. Signal identification of IoT gadgets utilizing watermarking is performed in two different ways with the end goal; one being static and the other is dynamic watermarking. In the static approach, identification of signals and intruders was finished with spread spectrum watermarking (Baheti and Gill, 2011). In this technique, if cyber-attackers begin to attack sensitive data of an organization, they acquire the information on static bit stream of signals. While dynamic identification of attackers and identification of signals was done with the help of deep learning. Established on this approach, this algorithm creates bit streams progressively which take care of the issue of eavesdropping attacks.

CLASSIFICATION OF INTELLIGENT IOT DEVICES: SMARTNESS OR INTELLIGENCE?

The ideology of “Smartness” or “Intelligence” lies at both macro and micro planes of IoT. These phrases might seem like a rush of self-driving cabs and smart refrigerators, yet it refers to a lot bigger than that. Presently, smart products/devices are generally worried about data, gadgets, and internet accessibility. The information should be analyzed to draw out the hidden bits of information; this should be possible with the assistance of Big Data Analytics. In the end, it is the research of this huge data with machine learning and artificial intelligence that makes the entire framework smart and truly efficient.

Table 1 should make the idea clear with regards to the level machine learning is turning out to be one of the greatest possibilities of smartness. It has demonstrated several instances of existing creatures whose intelligence has been imitated by a few artificially developed machines/software. These machines are or shall be equipped for carrying out specific tasks similar to the corresponding creature or are designed to have some comparative attributes. However, absolute imitation of the corresponding amount of qualities of the living being isn’t accomplished yet, but field experts are working and progressing towards making these machines act similarly to the corresponding living beings (Donepudi, 2019).

Moreover, it is observed that certain specific qualities and behavior are to be incorporated into these machines in order to make them fairly “smarter”. The way of thinking that enables machine learning is to make the logical models autonomous and empower ML to constantly learn and train its models from accessible information. This information must be stored and monitored continuously in order to be managed properly without any data loss. Nonetheless, a ton of information is produced every second on the internet, hence, all of that information may not be valuable enough to be used in the training. The trick here is to identify, analyze, and collect relevant information and leverage it effectively.

Table 1: List of Artificially Intelligent Machines Corresponding to their Living Counterparts

Skill Level	Living Being	Machine Example
Adaptive learning of new methods	Earthworm	AI-based intelligent thermostats
Learning through trial and error	Fish	CRONOS Robot
Learning through setting up a goal, achieving it, and later on evaluating it-self	Octopus	Cog
Self-awareness and Superior ideas	Chimpanzee	Siri
Has tender emotions like happiness and sorrow	1-6 years old children	Cozmo
Has a decent range of feelings, able to understand emotions and respond back accordingly	7-12 years old children	Pepper
Has a wide scope of feelings, interpret emotions, and respond back accordingly	12+ years old humans	MIT's AIProgram (Eugene Goostman)

Security Concerns in the Intersection of IoT, ML, and AI

Ensuring strong security measures helps keep information hidden, limits access to gadgets and resources stored on cloud platforms, offers secure approaches to connect with the cloud, and reviews gadget usage. An IoT security methodology decreases weaknesses using solutions like device identification management, encryption, and access control. Experts have clarified how IoT turns into a value however huge amount of information expanded its complications in identification, communication, regulation, and creating awareness. They additionally presented how the development of its information size on a real-time basis exceptionally affects the data and network weaknesses (Fadziso & Manavalan, 2017).

Security measures in the internally connected IoT frameworks, the security layers of communication mediums, and all the connections established amongst IoT frameworks within a network is a significant security risk and indispensable distress. Moreover, the real problem with devices connected to IoT frameworks is the design – which has been proven to be insufficient to deal with cyber-attacks and security threats posed by interconnected frameworks of devices. In this way, the entire IoT framework is left prone to security vulnerabilities. Field experts show their concerns over protection measures since almost every IoT gadget comes along with a lack of security protection and, hence, presents an easy way for cyber-attackers to attack their targets. Ensuring the security of 4V's of big data; velocity, variety, volume, and value will be a critical challenge (Bynagari & Fadziso, 2018).

Additionally, gadget identification is another security challenge. This identifier identifies specific codes and identification codes for specific gadgets, similar to the IMEI number for your phone. In any case, that isn't the case with all products connected to the IoT network. Henceforth the current recognizable proof guidelines will work for every gadget in the framework. Geo-Location is one more fundamental part of giving the right sort of safety in which we know the specific and actual location of the gadget. While we can extract such data from a smartphone or smart TV, it isn't the case with all gadgets connected with an IoT network.

At long last, Leads Access to different gadgets could give easy access to cybercriminals, and they could rapidly access other connected frameworks in the network is a huge security hazard. For instance, a simple exchange between a monitor connected with the IoT network would give easy access to cybercriminals to different other gadgets, including connected vehicles, smart home appliances, smart TVs, and so on. To mitigate the previously mentioned risks and challenges, IoT Security needs artificial intelligence (AI) and machine learning (ML) as a security tool to ensure elevated security layers.

INTERNET OF EVERYTHING (IOE)

Typically a lot of readers get confused with regards to the ideas of IoT (Internet of Things) and IoE (Internet of Everything). As explained by Cisco (Donepudi, 2015), the IoE is an intelligent connection established among processes, people, information, and objects. The motivation behind IoE lies in the connection of physical objects to virtual objects into a single entity. It is not only about enabling smart devices to send signals to each other or communicate through some mediums; it is about enabling a whole ecosystem of living, non-living, or any virtual service or product to communicate with one another. This digital part is absent in the idea of the Internet of Things. Internet of Things might have smart devices (connected to various sorts of things and people) and availability of an internet connection, however, it does exclude a digital aspect (sort of a digital object practically equivalent to any real-world object). Whereas, in the Internet of Things, the network of connections may vary from physical-physical, human-human, digital, human-physical, physical-digital, human-digital. Nonetheless, both these ideas are very similar yet somewhat different due to some distinct attributes i.e. digital presence. To improve clarity on the ideas, we depict these explanations through a Venn diagram in Figure 1.

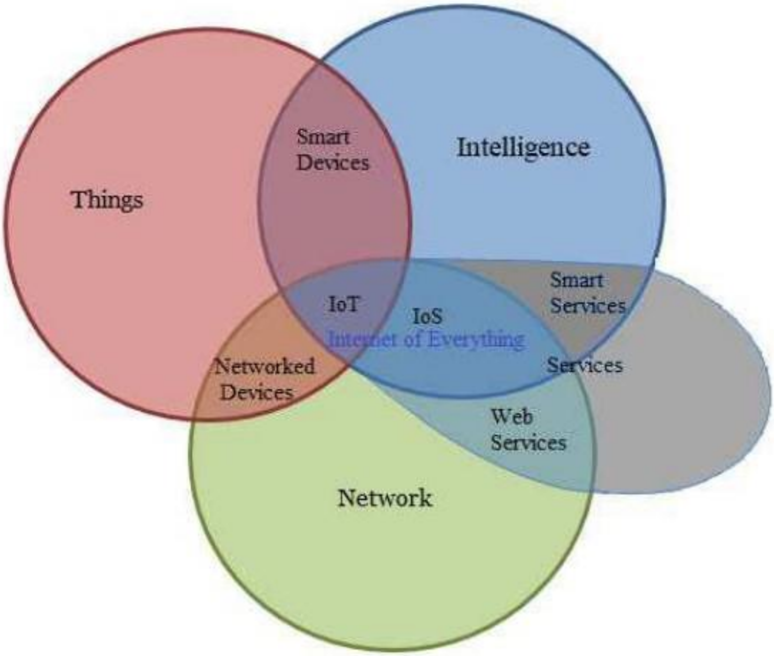

Figure 1: A Representation of Internet of Everything via Venn diagram

IoE has transformed into an expression to portray the integration of different networks and AI to basically all the objects, be it digital or physical, with a particular ultimate objective to enable them with extraordinary features. For instance, a website that might feature a smartly embedded system to figure out when an individual is irritated by a constant warning or getting enticed by an offer. Suppose a client-oriented portal; various users come across different designs/representations of a similar layout. Later on, we may likewise have the option to develop online offices so that even the crippled could utilize the Internet to their advantage. Then, at that point, only the genuine motivation behind the Internet would be achieved. Internet was designed for everybody and everything. To accomplish this objective, there lies the dire need to acknowledge and understand key ideas that form these firm ideologies.

Cyber-Physical Systems (CPSS)

The expression "Cyber Physical Systems (CPS)" came into the scene when it was suggested by Manavalan (2019). These systems are designed frameworks developed and based on the consistent integration of digital components and algorithms. In today's world, these systems are considered as a standard that's operated through computer-based tools. These tools are firmly connected through the internet and are effectively available to the public.

Wiener, during World War II, had installed a tech in anti-craft weapons that can automatically point and shoot. Regardless of the components he used did exclude cutting-edge equipment, his logic was viably a high-functional algorithm, yet one of those did include some digital components such as circuits and mechanical hardware. This idea had been a need of the hour due to the data-driven methodologies applied by the modern world. Not a long time back, people just used to imagine automated vehicles; today, people are developing automated vehicles with cutting-edge technologies to assist with mitigating road accidents. In order to take this solution further, street frameworks may likewise be integrated within the vehicles with the help of internet connectivity and provide real-time data to assist with avoiding accidents, overflowing traffic, and so forth. These frameworks can also be connected with police headquarters, medical clinics, etc.

In the recent scenario of developments, such systems are on the rise due to effective integration of multiple systems, smart products, installed computational gadgets, people and environments regularly connected through a correspondence medium. Such integrated systems include smart industry factories, cities, grids, buildings, homes, and cars where all of these are interconnected within a single ecosystem. These frameworks are designed to provide a highly adaptable, smart, and proficient solution. Let's assume a scenario where a road accident has taken place and the patient is rushed to an emergency clinic only to be asked to file a police complaint first. Wouldn't it be a smarter option to interconnect all the required frameworks? This way all the necessary information and details about the accident would be easily shared with the authorities. Each one of the fundamental steps would be followed right away and chances of delay in the treatment of that patient would be severely reduced.

Artificial Intelligence & Machine Learning as a Tool for Internet of Things

The highly saturated presence of smart devices has come along another era of transformation in the present-day world. The current scenario of interconnected gadgets in each family is very likely at a drastic rate, and the requirements for having a more solid network safety framework to deal with and relieve the danger against the information very still, information is used, and information surfacing, has been one of the major and basic security needs. Additionally, a higher level of safety prerequisites for IoT data collection, its data exchange timeframe, and the cloud platforms where the information storage and analysis occurs, reach the most elevated level (Donepudi, 2016).

Given its highly versatile digital framework nature and having as many interconnected gadgets where its information movement and analysis occur in a very complicated wide area network, the application of various AI tools have been extremely basic and taken advantage of to convey more practical detection and prevention systems. Numerous organizations are deploying Artificial Intelligence (AI) and taking advantage of Machine Learning algorithms as a piece of their risk management tool to have a solid digital protection framework to reduce the danger targeted on their organization's frameworks.

The inadequacy of traditional security strategies which are mostly rule-based has led fundamentally to see AI filling in as the main workaround of digital protection. As of now, AI is providing organizations to have tremendous security control support in proceeding with cyber-attacks. Given all the IoT data storage and data processing that happen on the cloud platforms, cloud security is another vital concern. Despite the fact that AI isn't bulletproof, its application as a service of digital protection frameworks is turning into a default standard and contributing massively at a significant level. Among the significant advantages that AI/ML convey include but are not limited to: weaknesses related to real-time and existing reporting, data analytics, detection of risky cyber-attacks, and alert frameworks.

Threats and Challenges of AI/ML in IoT

In spite of the fact that artificial intelligence and machine learning have drastically improved the IT landscape and security practices, these innovations have also posed some serious security concerns and offered an opportunity for hackers to develop and deploy a completely altered algorithm to carry out their vicious activities and lead serious cyber-attacks. Cyber attackers are working to research and develop some modern malware software that adjusts itself to the new parameters and leverages it to carry out malicious operations. Besides, hackers could apply these approaches to evaluate similar malware and upgrade its effectiveness to be able to penetrate their target's computer equipped with a primary machine learning algorithm. The more the malware is tested and trained, the higher will be data loss.

Multiple disadvantages posed by these innovations further include a higher cost of money, creativity limitation, partial capacity to imitate humans, loss of jobs for a lot of people, the requirement for human intervention to perform various tasks, and responding affirmatively to cyber attackers. Its effectiveness is highly dependent upon the precision and training of information obtained by various data streams. It needs visualization and improvement therefore it requires heavy datasets even with some significant learning experience.

Digital transformation is moving ahead in a more modern way presenting the high potential for malicious software and hackers to intrude the targeted systems connected with IoT devices or present external opportunities for people who can definitively exploit and corrupt the training datasets to develop algorithms that have adverse impacts and hazardous aftereffects that are truly challenging to identify and practically difficult to get hold of.

Future Work and Conclusion

Artificial Intelligence, Machine Learning, and the Internet of Things are just like three siblings if leveraged properly, we can accomplish amazing things in the future. The only thing is we need to take preventive measures in identifying the security and legitimate gaps of it and work on its better use cases and frameworks while intersecting these three. In a scenario where we need to accomplish financial as well as technical advantages through IoT is a difficult task. The absence of substantial goals and principles is disturbing. The headway of digitization and IoT puts new requirements on both the users and vendors alike. Small as well as large-scale organizations are not clear as to what domains will be changed with the implementation of an AI-based IoT methodology.

In most of the cases, plainly characterized, clear objectives are missing. When we take a look at modern organizations producing a huge number of datasets consistently; we're usually the organizations that neglect to completely collect, store, analyze and utilize such information to further develop process effectiveness or meet different objectives. Besides, the vast majority of the vendors are unable to explain, in substantial terms, to the customer how to reasonably make a helpful impact on business activities with IoT applications. Simply proposing cloud-based IoT platforms is not sufficient anymore.

The world is going towards a trap where a conversation about IoT rotates around technical terminologies rather than business objectives. Inventive thoughts need to be presented by the customers and they should be daring enough to contain the digital transformation brought about by this paradigm shift. In reality, vendors need to improve their operational activities in explaining what organizations can understand using IoT, and will be willing to assist with identifying business opportunities and set reasonable objectives.

To sum it all up, there are advantages and disadvantages to each disrupting innovation, and AI is no exemption from this list. What matters the most is that we recognize the challenges that lie before us and identify our obligation to ensure that we can take fair advantages while limiting the drawbacks. The robots are coming whether we like it or not. The least we can do is to allow this change to take place peacefully.

References

Baheti, R. and Gill, H. (2011). The Impact of Control Technology. Cyber-Physical Systems, 12, 161–166.

Bynagari, N. B. (2018). On the ChEMBL Platform, a Large-scale Evaluation of Machine Learning Algorithms for Drug Target Prediction. *Asian Journal of Applied Science and Engineering*, *7*, 53–64. Retrieved from https://upright.pub/index.php/ajase/article/view/31

Bynagari, N. B. (2019). GANs Trained by a Two Time-Scale Update Rule Converge to a Local Nash Equilibrium. *Asian Journal of Applied Science and Engineering*, *8*, 25–34. Retrieved from https://upright.pub/index.php/ajase/article/view/32

Bynagari, N. B., & Amin, R. (2019). Information Acquisition Driven by Reinforcement in Non-Deterministic Environments. *American Journal of Trade and Policy*, *6*(3), 107-112. https://doi.org/10.18034/ajtp.v6i3.569

Bynagari, N. B., & Fadziso, T. (2018). Theoretical Approaches of Machine Learning to Schizophrenia. *Engineering International*, *6*(2), 155-168. https://doi.org/10.18034/ei.v6i2.568

Donepudi, P. K. (2014). Technology Growth in Shipping Industry: An Overview. American Journal of Trade and Policy, 1(3), 137-142. https://doi.org/10.18034/ajtp.v1i3.503

Donepudi, P. K. (2015). Crossing Point of Artificial Intelligence in Cybersecurity. American Journal of Trade and Policy, 2(3), 121-128. https://doi.org/10.18034/ajtp.v2i3.493

Donepudi, P. K. (2016). Influence of Cloud Computing in Business: Are They Robust?. Asian Journal of Applied Science and Engineering, 5(3), 193-196. Retrieved from https://journals.abc.us.org/index.php/ajase/article/view/1181

Donepudi, P. K. (2018). AI and Machine Learning in Retail Pharmacy: Systematic Review of Related Literature. *ABC Journal of Advanced Research*, *7*(2), 109-112. https://doi.org/10.18034/abcjar.v7i2.514

Donepudi, P. K. (2019). Automation and Machine Learning in Transforming the Financial Industry. *Asian Business Review, 9*(3), 129-138. https://doi.org/10.18034/abr.v9i3.494

Fadziso, T., & Manavalan, M. (2017). Identical by Descent (IBD): Investigation of the Genetic Ties between Africans, Denisovans, and Neandertals. *Asian Journal of Humanity, Art and Literature*, *4*(2), 157-170. https://doi.org/10.18034/ajhal.v4i2.582

Lee, E. A. and Seshia, S. A. (2016). Introduction to Embedded Systems: A Cyber-Physical Systems Approach. MIT Press.

Manavalan, M. (2018). Do Internals of Neural Networks Make Sense in the Context of Hydrology? . *Asian Journal of Applied Science and Engineering*, *7*, 75–84. Retrieved from https://upright.pub/index.php/ajase/article/view/41

Manavalan, M. (2019). Using Fuzzy Equivalence Relations to Model Position Specificity in Sequence Kernels. *Asian Journal of Applied Science and Engineering*, *8*, 51–64. Retrieved from https://upright.pub/index.php/ajase/article/view/42

Manavalan, M., & Donepudi, P. K. (2016). A Sample-based Criterion for Unsupervised Learning of Complex Models beyond Maximum Likelihood and Density Estimation. *ABC Journal of Advanced Research*, *5*(2), 123-130. https://doi.org/10.18034/abcjar.v5i2.581

Manavalan, M.. (2019). P-SVM Gene Selection for Automated Microarray Categorization. *International Journal of Reciprocal Symmetry and Physical Sciences*, *6*, 1–7. Retrieved from https://upright.pub/index.php/ijrsps/article/view/43

Neogy, T. K., & Bynagari, N. B. (2018). Gradient Descent is a Technique for Learning to Learn. *Asian Journal of Humanity, Art and Literature*, *5*(2), 145-156. https://doi.org/10.18034/ajhal.v5i2.578

Yang, L. T., Di Martino, B., and Zhang, Q. (2017). Internet of Everything. Mobile Information Systems, vol. 2017.

--0--

Online Archive:

https://i-proclaim.my/journals/index.php/gdeb/issue/archive