Bringing Things to Life - The Power of Artificial Intelligence in IoT

[1]Mr.M.Venkatachalam, [2]Ms.K.Kalpana and [3]Ms.S.Vinciya Mary
[1]Assistant Professor, Department of Computer Science and Engineering,
[2,3]UG Student, Department of Computer Science and Engineering,
Sri Bharathi Engineering College for Women, Kaikurichi, Pudukkottai – 622 303.

Abstract: **The landscape of the Internet is undergoing a continual transformation, transitioning from the Internet of Computers (IoC) to the era of the "Internet of Things (IoT)." This evolution is giving rise to intricately connected systems, commonly referred to as Cyber-Physical Systems (CPS). These systems are formed through the integration of various elements such as infrastructure, embedded devices, smart objects, humans, and physical environments. The trajectory we are on is leading us towards an extensive "Internet of Everything" within a Smart Cyber-Physical Earth. The synergy of IoT and CPS, coupled with the field of "data science," holds the potential to usher in the next era of the "smart revolution." However, a significant challenge lies in effectively managing the vast amount of data generated, given the limitations of current computational power. Ongoing research in data science and artificial intelligence (AI) is diligently working to address this challenge. The convergence of IoT with AI could represent a monumental breakthrough. It goes beyond mere cost savings, the implementation of smart technologies, or the reduction of human effort—rather, it seeks to enhance the overall quality of human life. Despite the promises of advancement, critical concerns like security and ethical considerations continue to cast a shadow over the IoT landscape. The true essence lies not only in the allure of IoT with AI but in how the general populace perceives it—whether as a blessing, a burden, or a potential threat.**

Keywords: Artificial Intelligence, Internet of Things, Intelligent Systems, Datascience.

Introduction

The allure of the term "smart" captivates our imagination, yet the reality falls short of human-level intelligence. Take the example of smartphones – while they bear the label "smart," their autonomy remains limited. Consider the scenario where a smartphone, despite its intelligence, cannot automatically switch notifications to 'silent mode' when the owner is driving, showcasing a need for a more sophisticated level of automation. True intelligence, in this context, would involve wireless connections between individuals, their smartphones, and vehicles to enhance safety and reduce distractions.

In another instance, envision a situation where the owner falls ill. A truly smart phone would autonomously initiate an emergency call to a family member or nearby hospital, requiring seamless connections and pertinent information. This interconnectedness extends beyond smartphones – practically everything in the physical world requires connections to fulfill diverse needs. To achieve this level of intelligence, the integration of artificial intelligence (AI) is imperative.

AI, aiming to imbue computers with human- like reasoning, serves as a catalyst for the digital transformation of industries. Whether it's humans, animals, plants, machines, or inanimate objects, connecting and enabling them to make "smart decisions" can create an autonomous world. The realization of autonomy necessitates in the incorporation of machine learning (ML) to mimic human learning and a data analysis (DA) module to assess and analyze the data generated over time for enhanced efficiency.

This trend is gaining momentum, with efforts directed at integrating ML and DA into sensors and embedded systems of smart systems. The technology behind AI poses intriguing possibilities, challenging our preconceptions about the meaning and purpose of life and work. The rapid evolution of ML and DA within AI prompts a need for discussions on emerging trends, challenges, and potential threats.

Central to this transformative trend is the Internet of Things (IoT), envisioning a world teeming with intelligent devices, often termed "smart objects," interconnected through various communication mediums such as the Internet, Bluetooth, or infrared.

The Internet of Everything extends this idea, suggesting connectivity between every conceivable object, living or virtual. When applied to the physical world, these concepts manifest as Cyber-Physical Systems (CPS), creating a data-rich environment from which valuable knowledge can be extracted.

In managing this wealth of data, disciplines like Database Management System (DBMS), Pattern Recognition (PR), Data Mining (DM), Machine Learning (ML), and Big Data Analytics (BD) must evolve with improved methods, often overlapping in their scope. This article delves into insights, challenges, and applications of artificial intelligence within the realms of the Internet of Things, Cyber-Physical Systems, and the Internet of Everything.

Artificial Intelligence

Artificial Intelligence (AI) represents the scientific endeavor to impart cognitive abilities to machines, enabling them to perform tasks traditionally within the realm of human intelligence. AI systems are rapidly advancing in terms of application, adaptability, processing speed, and capabilities, gradually assuming less-routine tasks. Unlike human intelligence, which involves making perfect decisions at the right moment, AI focuses on choosing the right decision at the appropriate time. While human ingenuity continually reshapes the role of productive work, AI systems efficiently reduce the repetition of human efforts, delivering results in a comparatively shorter timeframe. Many ongoing AI initiatives fall under the category of 'Narrow AI,' enhancing specific tasks through technology. However, the overarching aim is to achieve something more comprehensive, prompting various fields to collaborate in driving AI development.

A convergence of disciplines such as philosophy, computer science, mathematics, statistics, biology, physics, sociology, and psychology has contributed to the interdisciplinary nature of AI. Intelligence, emanating from data generated across these domains, requires careful analysis to unveil underlying principles. Human brains are adept at this, but the process is time-consuming due to the unwelcome properties of real-world data, including its huge volume, unstructured nature, varied sources, need for real-time processing, and continuous changes.

To efficiently utilize data, AI heavily relies on data science techniques, which involve developing tools and methods to analyze large volumes of data and derive meaningful information. Drawing inspiration from computer science for tool development and incorporating methodologies from both basic and social sciences for analysis, data science encompasses a range of techniques, including pattern recognition, machine learning, data mining, database management systems, and big data analytics. Machine learning (ML) emerges as a key tool for achieving artificial intelligence.

Smartness or Intelligence

Intelligence in the realm of the Internet of Things (IoT) operates on both microscopic and macroscopic scales. While the notion may conjure images of futuristic talking refrigerators and self-driving taxis, its implications extend beyond mere novelty. Presently, the focus of smart objects mimics the natural learning process observed in humans, animals, and even plants. It occurs through supervised, reinforcement, and unsupervised learning, with additional methods like semi-supervised, active, inductive, deductive, and transfer learning. The ultimate goal is not consciousness but designing algorithms that enable machines to learn autonomously.

Learning involves acquiring or improving behaviors, skills, values, and preferences, with ML enabling machines to adapt to their environment and make independent decisions. The IoT scenario, characterized by overwhelming data volume, variety, velocity, and complexity, makes explicit programming impractical. ML, with its emphasis on implicit learning skills, enables machines to teach themselves, contributing to the concept of smartness in Cyber-Physical Systems (CPS) or IoT.

Machine learning, integral to achieving artificial intelligence, revolves around the idea that machines should learn from data. The recent advancements in AI owe much to the transformative perspective brought about by ML. Consequently, ML deserves credit for instilling smartness in machines as we collectively move toward creating human-like AI at an accelerated pace.

It revolves around data, devices, and connectivity. The analysis of this data is crucial for uncovering concealed insights, a task facilitated by Big Data Analytics (BDA). Ultimately, it is the fusion of big data analysis and machine learning that imbues the entire system with intelligence.

Internet of Things

A mere few decades ago, the notion of engaging in a video chat with family members on a different continent seemed beyond imagination. Today, it has become a commonplace occurrence. This transformation can be attributed to the increasing affordability of technology and the emergence of devices with enhanced capabilities. Everyday tasks, from sending emails to paying bills, transferring money, or booking a cab, can now be accomplished with a simple click on a smartphone.

The concept of the 'Internet of Computers (IoC)' has been in existence since 1991, gradually expanding as more individuals adopted its use. The evolution continued with the introduction of pocket phones and interconnected devices, giving rise to the 'Internet of Devices.' This network expanded further as mobile phones, computers, laptops, and tablets became more affordable and accessible to the common man. Gartner, Inc. predicted a substantial growth, forecasting that 6.4 billion connected devices would be in use worldwide in 2016, a 30 percent increase from 2015, and anticipating a staggering rise to 20.8 billion by 2020 [24]. In 2016 alone, over 5.5 million new devices were connected daily, signifying the vast potential of the Internet of Things (IoT).

As various entities continue to connect and form the IoT, it encompasses a multitude of disciplines. Therefore, the IoT can be perceived as a convergence of diverse domains. Figure 1 provides a representative list of some of these domains, which often overlap in terms of concepts and techniques. Essentially, the Internet of Things is a connected system comprising physical entities such as appliances, crop fields, plants, animals, and humans. Humans connect to these devices through smart objects attached to both, capable of sending, receiving, and analyzing data. These smart objects serve as representatives of the entities they are attached to within the network."

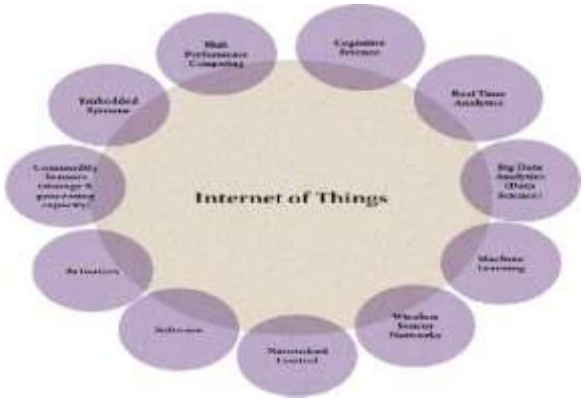

Fig. 1: Different fields merging into IoT

Things and Everything

When we are talking about IoT and IoE, we must be very clear about the concept of "things" and "everything". One straightforward con- cept that may come to mind is anything that can be connected may be the "thing" in IoT. However, we define it other way round. There can be more features in making a physical object a "thing". The "thing" (living or non-living) should have:

1. a way to generate or collect data,
2. a way to process data,
3. a way to send or receive data,
4. a way to identify itself.

The main concept to consider, when thinking of IoT, is that "Things" are physical objects, i.e., anything that has a real life pres- ence. The Internet as we know it is not just made of physical devices. For instance, a website cannot be thought to be a physical entity; it exists somewhere virtually. This is true for services that we might use every day, such as online shopping sites, social media sites, etc. These "intelligent services" along with the "things" make the "every- thing". Thus, inter- connections as well as intra-connections between "things" from physical world and "intelligent services" from the cyber world make the IoE.

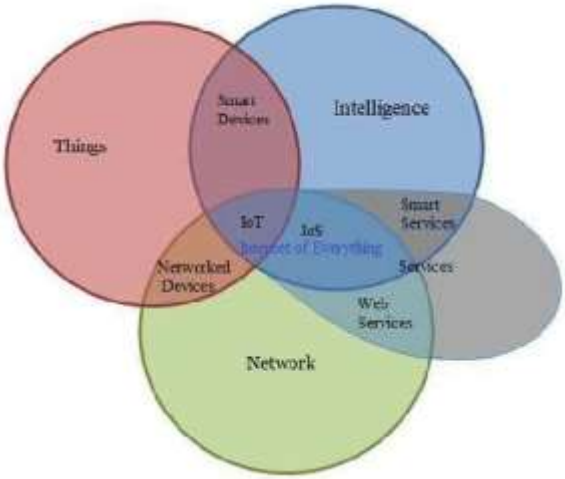

Fig. 2: A Venn diagram for the concept of Internet of Things (IoT), Internet of Services (IoS) and Internet of Everything (IoE)

AI enabled IoT

The Internet of Things (IoT) is a comprehensive concept that involves an array of sensors, actuators, data storage, and data processing capabilities interconnected through the Internet. Consequently, any IoT-enabled device has the ability to sense its environment, transmit, store, process gathered data, and take appropriate actions.

The effectiveness of an IoT service in exhibiting true smartness is contingent upon its processing and action capabilities. An IoT system lacking smartness will have limited functionality and an inability to adapt with evolving data. Conversely, a more intelligent IoT system incorporates artificial intelligence (AI), serving the primary goals of automation and adaptation.

In this context, several examples of existing IoT services leveraging AI are explored:

1. Voice Assistants:

Alexa: Amazon's voice assistant utilized in products like Amazon Echo and Amazon Tap. Customizable through the Alexa Skills Kit (ASK).

Siri: Apple's voice assistant employed in Apple Homepod for similar purposes.

Google Assistant: Used in Google Home, capable of recognizing up to six different users.

These voice assistants perform various tasks through continuous application of AI subfields, including automatic far-field voice recognition, wake word detection, natural language processing, contextual reasoning, and more.

2. Robots:

Pepper (SoftBank Robotics): A humanoid companion robot capable of understanding human emotions and interacting with humans in commercial settings.

Sophia (Hanson Robotics): A social humanoid robot with human-like expressions, citizenship, and the ability to engage in interviews and music performances.

Robotic Kitchen (Moley Robotics): An advanced robot integrated into a kitchen, capable of preparing expert-quality food.

Robots, with their sensors, actuators, and AI, continuously learn and adapt, mimicking human interaction.

3. Smart Devices:

Smart Oven by June: Utilizes HD cameras and a food thermometer for precise cooking, operable through voice commands via Alexa.

SkyBell (Honeywell): An HD WiFi doorbell allowing remote interaction through smartphones or voice assistants, enhancing home security.

Smart Lights by Deako: Internet-connected lights controllable remotely, receiving software upgrades for added functionality.

Automotive AI by Affectiva: In-cabin sensing AI for emotional and cognitive state detection in robo-taxis and highly automated vehicles.

4. Industrial IoT:

Primer (Alluvium): Offers real-time Stability Score analysis for industrial solutions, aiding in early issue detection and decision-making.

Plutoshift: Enables continuous tracking of asset performance, financial impact measurement, and support for informed decision-making in industrial sectors.

Combining AI and IoT enhances opportunities and potential, as machine learning (ML) and big data analytics (BDA) extract valuable insights from IoT-generated data. AI is crucial for interpreting the vast amount of data, allowing IoT systems to evolve and adapt to new patterns autonomously. The synergy between AI and IoT holds immense promise for the future.

Components of IoT-CPS

Having established a clear interrelationship between IoT, CPS, and associated terms, the pivotal focus shifts to the ecosystem of these technologies. Given that CPS is an amalgamation of subsystems, our attention can be directed towards the structure and components of IoT initially. Breaking down the various elements of IoT, we unveil a composition depicted in Figure 3.

Figure 3 delineates several components within an IoT system. Beyond network infrastructure and security, a substantial aspect of IoT necessitates data storage and processing on both a macroscopic (i.e., within the overall system) and microscopic level (i.e., within each smart object locally). Smart objects themselves must possess data processing, intelligence, and decision-making capabilities. To achieve this, built-in data processing tools are imperative for analyzing sensor data and making informed decisions. Machine learning and data analytics emerge as optimal candidates for such intelligent data analysis. On a macroscopic level, billions of things generate data independently, transmitted over the network to remote data storage locations for real-time data analysis, resembling a significant big data task.

The continuous generation, storage, and processing of substantial data make big data analytics (BDA) and machine learning (ML) integral in shaping the intelligence within IoT.

Moreover, smart objects can boast limited data storage and processing capabilities. For instance, a smartwatch prompts the user to walk when it detects prolonged stationary periods (sitting or lying down), yet refrains from alerting during sleep. It can distinguish between sleep and sedentary states without transmitting data to external servers, conducting local analysis to trigger the alarm. These short-term decision-making capabilities are embedded in smart devices.

For long-term decision-making or gaining insights, remote storage and processing may become requisite.

As IoT entails myriad connected devices, establishing an "everything to everything" connection saturates the physical world with sensors/actuators while inundating the virtual world with data. The ensuing network complexity perpetually generates data throughout the CPS. Distinct analyzing systems handle different facets of the IoT- CPS, prompting the extraction and processing of smaller relevant data portions when necessary. Real-time analysis becomes crucial for making practical decisions, and the data management within IoT is inherently distributed across its individual components, collectively forming a comprehensive system. Subsequent sections delve into the particulars of these IoT components.

Smart Objects

To comprehend such a substantial concept, we'll need a multitude, numbering in the millions or more, of smart objects that generate data. These smart objects serve as the fundamental building blocks of this extensive system. Within the physical realm, two key elements must be considered: a Physical Entity (PE) and a Smart Object (SO).

A Physical Entity (PE) encompasses entities such as people, creatures, and plants that may not directly interface with the IoT but are integral components of the system. These physical entities have smart objects (SOs) attached to them, representing AI elements with the ability to communicate via the network. These SOs can take various forms, including implanted chips, wearables, or smartphones somehow attached to the PE. Therefore, an SO becomes the device facilitating the connection of a PE to the virtual 'Internet' of things.

As the Internet is virtual, both the PE and SO, being physical objects, require a digital representation. The digital entity (DE) serves as the digital representation of the PE by the SO. For instance, if we consider ourselves as the PE, our smartphone becomes the SO, and our social media app becomes the DE.

SOs are the physical world representation of DEs in the digital realm, possessing the capability to sense, store, process (locally), and communicate via networking. SOs may act as intelligent agents with some level of autonomy, cooperating with other entities and exchanging information with human clients and other computing devices within interconnected Cyber-Physical Systems. DEs, on the other hand, are virtual programming elements with autonomous objectives, which can be services or simple coherent data entries.

In the cyber world, a Physical Entity (PE) or thing can be represented by a Digital Proxy (DP). DPs can be likened to users in the cyber world, much like social media profiles (our DP) are perceived as representing us (where we are the PE). Each PE has a DP, used to portray it in the digital world. There are various forms of digital portraits, known as DE, that we can imagine, such as avatars, 3D models, objects (or instances of a class in an object-oriented programming language), and even a social network account.

However, in the context of IoT, Digital Proxies possess two fundamental properties:

Each Digital Proxy must have a unique ID distinguishing it from others, with the association between the Digital Proxy and the Physical Entity established automatically. Relevant digital parameters related to the characteristics of the Physical Entity can be updated upon any changes in the latter. Similarly, changes affecting the Digital Proxy 'might' be reflected on the Physical Entity in the physical world through actuators.

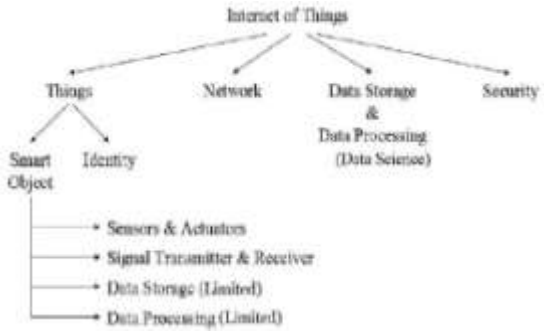

Fig. 3: IoT architecture tree

Data Storage and Data Processing

The primary goal of IoT and CPS is to establish an autonomous system capable of handling diverse situations globally, ultimately enhancing the quality of human life. The fundamental framework of IoT-CPS comprises smart objects, resembling nodes in a graph, and the connections between them. Once all nodes and connections are established, data is generated and communicated between nodes continuously. However, the challenge arises as smart objects (SOs) lack the knowledge of how to handle this data—they cannot store it, nor do they understand how to process it. Without proper data storage and processing units, the objective of autonomy, decision-making, and taking actions cannot be fulfilled. This crucial feature is required both locally within smart objects and globally across the entire system.

Smart objects handle small sets of continuously flowing data into the system, temporarily storing it until a task is completed, and then transferring it to the global data store. While the data store of the entire system may not receive streaming data, it mostly accumulates large chunks of collected data over time. To manage both types of data in real-time and utilize them effectively, the role of big data analytics becomes crucial.

While data needs to be stored, the processing phase poses the challenge of uncertainty regarding what exactly needs to be done. A smart IoT-CPS system is expected to operate autonomously, observing its surroundings through various parameters, learning from experiences, understanding the current needs, and making useful decisions or taking actions. To replicate human-like learning capabilities, the system must possess the ability to learn from data independently, especially in situations where human intervention may not be available or desired most of the time. Achieving these functionalities can be effectively facilitated with the integration of artificial intelligence.

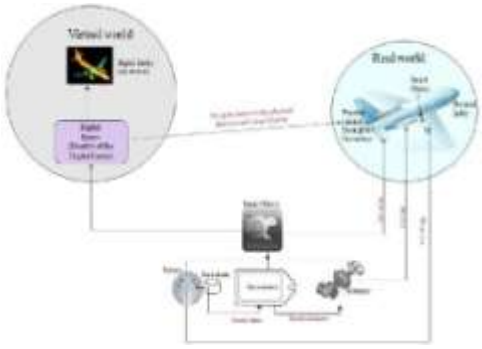

Fig: An example of real world to virtual world mapping

Security

While the prospects of IoT are intriguing, as Sarah Jeong highlighted in her book [31], it also carries the moniker "Internet of Garbage." She emphasizes that if the Internet were a city, its streets would be cluttered with undesirable elements such as harassment, crimes, copyright abuse, malwares, spams, and more. However, there is an opportunity to foster better interactions and discourse through thoughtful architecture, rigorous moderation, and efficient community management. The key is to filter useful content from the garbage and endeavor to find value in it.

As IoT becomes increasingly prevalent worldwide, it brings forth new demands, with security emerging as a paramount concern. Beyond assembling smart objects, implementing big data analytics, and establishing communication capabilities, the critical challenge lies in ensuring security in such a vast scenario. The security of IoT devices extends beyond the devices themselves; the software applications and network connections linking to these devices must also be secure. Users of smart objects and IoT are vulnerable as their data traverses a network. The primary issues revolve around data confidentiality, privacy, and trust. In IoT, users, along with authorized smart objects, access data, necessitating the ability to verify the entity's authorization through authentication and identity management.

The collective effort to protect interconnected systems and their components is commonly referred to as 'cybersecurity.' Cybersecurity plays a pivotal role in safeguarding smart devices, IoT, and CPS, preventing unauthorized access from within the devices and externally. Its objectives include protecting services, hardware resources, information, and data in both transition and storage. Various technologies, such as cryptographic systems, firewalls, intrusion detection systems, anti-malware software, and secure socket layers, contribute to the cyber security framework.

Ethical concerns also come into play, such as the scenario where a wearable gadget records a user's health and fitness information. This information may be accessible to gadget service providers, who might sell user data to other companies without consent. This practice can lead to personalized offers or advertisements based on the user's fitness tracker data, anticipating their potential interests. Some users may find this intrusive, while others may not mind promotional offers. However, the unauthorized sale or distribution of user data without consent is generally not in the user's best interest.

User consent should be a prerequisite for data sharing, ensuring that selling or distributing personal data occurs only with the explicit agreement of the user.

AI enabled IoT-CPS

In the realm of IoT-CPS, data is an indispensable component, whether it's vast or compact, playing a vital role in the interconnected world of devices. Smart objects should possess localized processing capabilities and inherent intelligence. However, for decisions reliant on data, a more extensive dataset is essential. Storing such data within a smart object might not always be feasible. This is where the macroscopic approach comes into play; data is transmitted to remote locations in a distributed manner and analyzed. The results of this analysis are integrated, and when necessary, decisions are sent back to the smart object for execution by the actuator. The time between data transmission and decision implementation must be practical; otherwise, it loses its meaning. Traditional analytic tools struggle to capture the entirety of this massive data in real-time. The volume, velocity, and variety are too extensive for comprehensive analysis, and the potential relationships and correlations between different data sources are too vast for manual comprehension by analysts.

An effective machine learning system dealing with big data requires data preparation capabilities, both basic and advanced learning algorithms, automation, adaptability, scalability, ensemble modeling, and real-time decision-making.

While machine learning systems have demonstrated the ability to let computers think on our behalf, addressing big data demands adaptation of existing ML methods and the development of new ideas.

CPS and IoT are fundamentally driven by the pursuit of social, economic, and human benefits. These technologies find applications in various domains such as personalized healthcare, smart grids, smart industries, and smart transportation. For instance, a smart industry can enhance manufacturing processes by sharing real-time information among industrial equipment, supply chains, distributors, business systems, and customers. In healthcare CPS, a smart hospital could remotely monitor patients' physical conditions, especially in hard-to-reach areas, enabling timely interventions during emergencies like road accidents. Quick notifications to the nearest hospital, police station, and family members, along with immediate dispatch of an ambulance and alerting the on-duty doctor, exemplify the potential benefits. Such interconnected autonomous systems are particularly advantageous in emergency situations, and the infusion of artificial intelligence amplifies the overall "smartness" in the IoT-CPS infrastructure.

Applications of IoT-CPS involve components interacting through a complex physical environment, presenting a challenging innovation that has the potential to transform various sectors, including manufacturing, energy systems, healthcare, transportation, critical infrastructure, emergency response, defense, and agriculture. Organizations embracing IoT-CPS should incorporate system-aware assets capable of autonomously assessing potential faults or failures in the system. System-awareness implies that a device embedded in any part of a machine should sense both itself and its environment. The integration of AI into such interconnected IoT-CPS scenarios propels us toward not just a smarter but a "brilliant planet."

Cognitive AI and IoT-CPS

IoT transcends the mere combination of wireless sensor networks, data storage, embedded systems, and security issues; it represents a vision of a world interconnected by intelligence. This may sound like science fiction, but it is the essence that makes IoT a prevalent term today. The conventional approach to programmable computing involves filtering information through a fixed set of rules to arrive at a result. However, this method proves inefficient in addressing the multifaceted aspects of a complex, fast-paced world where the information processing capability diminishes exponentially, leading to underutilization. Cognitive computing, in contrast, overcomes such limitations by learning from the intricate relations within connections involving people, things, the environment, and their interactions. Instead of being deterministic, cognitive frameworks are probabilistic, enabling them to keep pace with the volume, variety, variability, and unpredictability of data generated by the IoT.

Formally termed cognitive computation models, these frameworks constitute an integral part of the artificial intelligence in IoT-CPS. They possess the capability to comprehend the "unstructured" 80 percent of the world's information, including recordings, audio, blogs, images, emails, and tweets. This means that organizations can now illuminate aspects of the IoT that were previously imperceptible. When applied to the IoT, this cognitive understanding results in

what is known as Cognitive IoT—systems that integrate intelligence into, and learn from, the physical world.

"Cognition" refers to the process of acquiring knowledge and understanding through thoughts, experience, and senses. Intuitively, Cognitive IoT can be viewed as an extension of IoT that is capable of understanding, reasoning, and learning. While these three aspects of cognition share similarities between human cognition and Cognitive IoT, they carry nuanced meanings. For IoT, to 'understand' implies the ability to collect vast amounts of data from the network and discern the underlying meaning of the data, creating concepts, identifying entities, and defining relationships between them.

The ability to 'reason' means that IoT should be capable of providing appropriate answers to queries or solving relevant problems without explicit programming. Lastly, a cognitive IoT should be able to 'learn,' independently deriving new information from the available data using the past knowledge it has acquired.

AI enabled IoT-CPS

While machines are not designed to replace humans entirely, their purpose is to assist humans in reducing the task load. It is crucial to emphasize that humans should maintain supremacy over machines. Artificial Intelligence (AI) proves most effective when combined with human intelligence rather than replacing it. This underscores the concept that computers and humans possess different strengths in the vast realm of excellence: computers excel at arithmetic tasks and counting, while humans demonstrate remarkable performance in logic and reasoning. These distinct forms of intelligence complement each other rather than being diametrically opposed. AI, therefore, represents the technology that can fulfill the dream of having 'things' that can 'think' [32].

Several examples illustrate how artificial intelligence has been incorporated and utilized in the IoT-CPS scenario:

Energy Utilization: Algorithms have been developed on a small scale to reduce energy consumption in a coffee machine (ARIIMA). This approach can be adapted and implemented in various scenarios, such as temperature control systems in houses, making them more efficient and reducing wastage. The system learns and adjusts temperature settings efficiently based on residents' preferences.

Routing/Traffic: Machine learning is applied in traffic management and routing, considering parameters like traffic, road conditions, weather, etc., to suggest the best routes.

Cost Savings: Predictive abilities are invaluable in an industrial setting. Machine learning algorithms, drawing information from sensors on machines, can learn the usual running conditions. When irregularities occur, the system can identify the machine and raise an alarm, preventing accidents and saving costs. Companies like Augury use vibration and ultrasonic sensors to predict malfunctions and save money [33].

In essence, we aspire to achieve an 'Internet of Things' where both the 'Internet' and the 'Things' have the power to think [32]. This infusion of thought represents the 'intelligence' aspect of IoT. While this may seem overrated, it encapsulates the essence of current research in artificial intelligence.

Challenges

Once an idea is conceptualized, bridging the gap between the idea and a functional prototype poses significant challenges. The development of a working prototype requires substantial resources. Even with a prototype in place, the critical question remains: how can one ascertain the success or failure of this innovative technology? Often, both novices and experts in the domain make erroneous predictions. Recent trends in the Internet of Things (IoT) underscore the rapid influx of data from diverse sources in varied formats, surpassing the capabilities of information systems to absorb, store, analyze, and process it. While databases with petabytes of data are not uncommon, the primary goal is to extract meaningful information, such as patterns, structures, and underlying relationships. This task is intricate and demands advanced storage and processing techniques due to the unprecedented volumes of data.

In response to these challenges, new algorithms are being devised, and established techniques are being revisited and tailored in fields like Pattern Recognition, Machine Learning, and Data Mining. However, the convergence of IoT and Cyber-Physical Systems (CPS) raises additional concerns. The field of Artificial Intelligence (AI) requires further development to align with the emerging IoT-CPS infrastructure. Complex adaptive AI systems could potentially lead to self-sustaining malicious evolution, akin to cancerous growth in the human body. Research efforts are crucial to address these evolving AI systems with superior countermeasures.

Cybersecurity emerges as a major concern in this technological era, where the possibility of cyber wars looms. Autonomous systems are susceptible to malicious use if hacked, necessitating the identification and mitigation of vulnerabilities in AI systems. Mock attacks on AI systems can be developed to immunize existing safeguards. Proactive measures, such as predicting new types of attacks, must be integrated into organizational systems. Rapid recovery systems are essential for organizations to bounce back from cyber events disrupting regular business operations. It is imperative to automatically identify and safeguard critical information that could be maliciously exploited, even when shared publicly, and AI systems can play a role in ensuring privacy.

Conclusion

In the future, individuals will engage with intelligent devices, consume smart capsules capable of assessing the impact of medicine on the body, reside in intelligent homes, and more. While this may seem like science fiction, it represents the focal point of ongoing research. The vision is of an interconnected world where every facet is intelligent and linked to the Internet, culminating in what can be termed a 'smart cyber revolution.' Nonetheless, the trajectory prompts a debate on whether this shift is towards creative destruction.

As machines increasingly undertake less routine tasks, this transformation coincides with a period where many workers are already grappling with challenges. With appropriate policies, there is an opportunity to harness the benefits of automation without widespread unemployment. Human ingenuity will redefine the nature of productive work, emphasizing educational opportunities and fostering a workforce equipped with reskilling and upskilling.

Continuous deployment of AI models in real- world scenarios demands a reassessment of the impact of such automation on human life. While these systems offer myriad benefits, they also present inherent risks, including privacy breaches, the codification and reinforcement of biases, diminished accountability, hampered due process, and an escalation in information asymmetry between data producers and holders. The Internet of Things and Cyber-Physical Systems (IoT- CPS) constitute a diverse and intricate network, making it challenging to monitor every ethical or security breach incident. Failures or bugs in the software or hardware can have significant consequences, with even power outages causing inconvenience. Consequently, the implementation of an additional AI system, supervising the IoT's activities in real-time, may become necessary. In the future, we might envision a democracy of such systems, preventing irrational actions. As our lives become increasingly intertwined with technology, we must ensure that humans retain supremacy over the artificially intelligent landscape.

This approach is essential for managing and guiding the ongoing revolution without succumbing to technological enslavement.

References:

[1]. R. Baheti and H. Gill, "Cyber-Physical Systems," The Impact of Control Technology, vol. 12, pp. 161–166, 2011.

[2]. R. S. Michalski, J. G. Carbonell, and T. M. Mitchell, Machine Learning: Artificial Intelligence Approach. Springer Science & Business Media, 2013.

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

[4]. H. Witten and E. Frank, Data Mining: Practical Machine Learning Tools and Techniques. Morgan Kaufmann, 2016.

[5]. L. Monostori, B. Kádár, T. Bauernhansl, S. Kondoh, S. Kumara, G. Reinhart, O. Sauer, G. Schuh, W. Sihn, and K. Ueda, "Cyber-Physical Systems in Manufacturing," CIRP Annals, vol. 65, no. 2, pp. 621–641, 2016.

[6]. E. A. Lee and S. A. Seshia, "A Theory of Formal Synthesis via Inductive Learning," Acta Informatica, vol. 54, no. 7, pp. 693–726, 2017.

[7]. Q. F. Hassan, A. R. Khan, and S. A. Madani, Internet of Things: Challenges, Advances, and Applications. Chapman & Hall/CRC Computer and Information Science Series, CRC Press, 2017.

[8]. G. Fortino and P. Trunfio, Internet of Things based on Smart Objects: Technology, Middleware and Applications. Springer, 2014.

[9]. L. T. Yang, B. Di Martino, and Q. Zhang, "Internet of Everything," Mobile Information Systems, vol. 2017, 2017.

[10]. J. Kaplan, Artificial Intelligence: What Everyone Needs to Know. What Everyone Needs To Know, Oxford University Press, 2016.

[11]. N. Marz and J. Warren, Big Data: Principles and Best Practices of Scalable Real- Time Data Systems. Manning, 2015.

[12]. J. Leskovec, A. Rajaraman, and J. D. Ullman, Mining of Massive Datasets. Cambridge university press, 2014.

[13]. J. Holler, V. Tsiatsis, C. Mulligan, S. Avesand, S. Karnouskos, and D. Boyle, From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence. Academic Press, 2014.

[14]. M. M. Gorman, Database Management Systems: Understanding and Applying Database Technology. Elsevier Science, 2014.

[15]. S. Theodoridis and K. Koutroumbas, Pattern Recognition. Elsevier Science, 2008. [16]. N. Gershenfeld, When Things Start to Think: Integrating Digital Technology into the Fabric of our lives. Henry Holt and Company, 2014.

[17]. B. Guo, D. Zhang, Z. Yu, Y. Liang, Z. Wang, and X. Zhou, "From the Internet of Things to Embedded Intelligence," World Wide Web, vol. 16, no. 4, pp. 399–420, 2013.

[18]. C. Gomez and J. Paradells, "Wireless Home Automation Networks: A Survey of Architectures and Technologies," IEEE Communications Magazine, vol. 48, no. 6, pp. 92–101, 2010.

[19]. V. Coskun, B. Ozdenizci, and K. Ok, "A Survey on Near Field Communication (NFC) Technology," Wireless Personal Communications, vol. 71, no. 3, pp. 2259– 2294, 2013.

[20]. J. Fan, F. Han, and H. Liu, "Challenges of Big Data Analysis," National Science Review, vol. 1, no. 2, pp. 293–314, 2014.Ghosh, N. S. Mishra, and S. Ghosh, "Fuzzy Clustering Algorithms for Unsupervised Change Detection in Remote Sensing Images," Information Sciences, vol. 181, no. 4, pp. 699–715, 2011.

[21]. Halder, S.Ghosh, and A.Ghosh, "Aggregation Pheromone Metaphor for Semi-Supervised Classification," Pattern Recognition, vol. 46, no. 8, pp. 2239–2248, 2013.

[22]. D.Cohn, "Active Learning," Encyclopedia of Machine Learning and Data Mining, pp. 9–14, 2017.

[23]. S.Jha and S. A. Seshia, "A Theory of Formal Sync