

JUL-DEC 2021

**BULLETIN OF
INFORMATION
TECHNOLOGY**

BY DEPARTMENT OF INFORMATION TECHNOLOGY

BIT

**BULLETIN OF
INFORMATION
TECHNOLOGY**

DEPARTMENT OF INFORMATION TECHNOLOGY

AT THE EDITING DESK	5
CHALLENGES TO APPLICATION OF ARTIFICIAL INTELLIGENCE IN HEALTHCARE	7
CONFERENCE ROOM TO CONFERENCE CALL	10
EXPLAINABLE AI: INCREASING TRUST OF AI BLACKBOX	12
CYBORGS - THE FUTURE MAN KIND	15
WILL AI TAKE OVER THE WORLD	17
CYBER SECURITY	20
IMPACT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING ON TRADING	22
INTERNET OF THINGS	24
ARTIFICIAL INTELLIGENCE IN MEDICAL FIELD.	28
ABOUT THE DEPARTMENT	30

AT THE EDITING DESK

FACULTY ADVISORS

- Dr. Neeba EA | HoD
- Ms. Bency Wilson | Assistant Professor

STUDENT EDITORS

- Arjun Sunil Kumar | S7 IT
- Sonia George | S7 IT
- Meenakshi Venkat | S5 IT

EDITORIAL

CHALLENGES TO APPLICATION OF ARTIFICIAL INTELLIGENCE IN HEALTHCARE

BY DR. NEEBA EA | HOD

Artificial intelligence (AI) has far-reaching potential in the healthcare industry and in the aftermath of a pandemic, there could be no greater demand for its application. It possesses the ability to transform patient experience and bolster clinical practice as well as improve the pharmaceutical industry. Moreover, it can be applied to various levels of the supply chain, ranging from simple tasks, like medical review, to complex tasks like analysis of radiology images and therapeutic drug design. Routine tasks that are carried out manually can be shifted into the automatic mode, increasing productivity. Globally, there is an urgent need to improve patient care and the healthcare sector requires this to be carried out with less expenditure. AI provides this and empowers consumers to have control over their healthcare as well. Paving the way for AI would mean a healthcare sector that is more convenient, cost-effective, and efficient. It is, however, not without several challenges, such as availability of datasets, maintaining accuracy, data security and privacy, and long timelines for feedback.

The basis of AI's application in healthcare is to provide data-driven methodologies to address medical issues. For

example, deep neural networks, which are powerful in obtaining information from voluminous datasets, have significantly influenced precision medicine and medical imaging. Convolutional neural networks have been used in aiding clinicians classify melanoma, while machine learning is applied in the assessment of cardiovascular health and in the prediction of cardiovascular events.

AI depends on large datasets to make predictions and whilst the healthcare sector provides vast amounts of data, it is not without bias. During the pandemic, for instance, a form of bias was encountered - pulse oximeters, which measures oxygen saturation by sending infrared light through the skin, are affected by skin colour. The device was found to systematically overestimate oxygen saturation levels in non-Caucasian patients. This highlighted that medical decisions may be error-prone if the data provided to AI technologies is not inclusive. This kind of bias, i.e. where the distribution of a dataset is not representative of the true population, results in reduced diversity in clinical datasets and ultimately the AI may fail to provide adequate healthcare to all. This occurs because biomedical databases tend to have missing pieces of information. Therefore, if training data does not represent the population accurately, then the algorithmic bias is reinforced by the AI, which can have a detrimental impact on diagnostics and therapy. The need of the hour is to ensure that algorithmic bias is reduced through fairer open science practices. Bias can arise in any stage of the algorithmic development process. For example, most applications of AI include diagnostics, so if a diagnostic AI is trained only with a particular dataset, then it may fail to diagnose entire patient groups, e.g. gender groups.

Another challenge is the issue of data gaps. Several governments, institutions, and funding agencies have been working towards promoting open data sharing. The issue is that despite the increased number of repositories, the vast

majority is not comprehensive. For instance, there is a lack of genetic information, which hinders the development of biomarkers, which are used in diagnostics. In addition, there is also a certain degree of inconsistency in formatting and limited data disaggregation, which prevents these open datasets from being utilised to their full potential. This ultimately affects the quality and diversity of AI.

Another challenge is the lack of standardisation in data. Data can be published in incompatible formats, making their analysis and interpretation difficult. In addition, such variation limits the application potential of the algorithms they are trained with. Collectively, irregular data sharing and variation in data quality affects the quality of AI.

These challenges highlight the need for open science to be included in the AI design process. This includes, open sharing of healthcare data, incorporation of data standards to allow for interoperability, inclusion of synthetic data to overcome bias, sharing of source code, rigorous efficiency evaluation through testing, and the adoption of common metrics to determine AI reliability.

In order for AI technologies in healthcare to be beneficial it is necessary that they be accurate and representative. Implementing open science into AI design will allow for the generation of inclusive and diverse datasets, which ultimately forms the foundation of AI technologies and their ability to impart healthcare for all.

CONFERENCE ROOM TO CONFERENCE CALL

BY ARJUN SUNIL KUMAR | S7-IT

The year 2020 has brought a drastic change to the way we live our lives, in a matter of days our world changed in a way we thought could never happen. The pandemic forced people into their homes and has managed to keep them there for the near future. This meant that people in the industry could no longer work in a common space. The four walls of the conference rooms that once held meetings that could change peoples lives in a matter of hours, now remain empty. The inability to be in a common space forced people to move to alternatives where they could be in a single space but yet be miles away from each other, and that was the online meeting platforms such as Zoom, Cisco's Webex and Google's Meet. These platforms have revolutionised the way we conduct meetings, classes, lectures and communicate with each other. These platforms have existed for a few years now, but they became relevant to people only when they were confined to their homes and could no longer meet with people in person. In the world of technology theoretically speaking, nothing that is connected to the Internet is secure, that includes all of these meeting platforms. A standard conference room was in a way too basic to be insecure, any discussion or discussion that took place in the conference room never leaves the 4 walls of the conference room.

This calls into question how secure are these online meeting platforms and can they be trusted with the proprietary information that is discussed amongst the members who use these platforms for meetings. Ever since the surge in the popularity of online meeting platforms we have heard reports

of the lax security that these online platforms have and how information shared on these platforms could potentially be leaked. One of the common issues faced were the unauthorised entry of participants into a meeting, several issues were reported where people entered a meeting without the consent of the host due to certain security measures like waiting room being off. Some might say this is poor journalism as the host has the ability to turn it on when the meeting is scheduled. But sometimes some hosts are not aware of what each option is, which means they won't know what options are essential for them and which options to avoid.

The meeting platforms while having existed for so many years have never had such a large number of users or have heavy traffic like it does now. The security implications of online meeting platforms are a real threat to industry and government. Platforms like Zoom have also been berated for their poor privacy policy and data protection as it allowed them to use user information pretty much however they please.

6 Months into the pandemic, all tech giants and service providers have enhanced their security protocols in a significant manner to ensure the safety of their customers. Zoom for example has gradually improved and made certain features mandatory like meeting room password and waiting rooms. Google Meet is rolling out features that are focused on the education industry to all educational institutions to conduct online classes easily. The pandemic has forced a positive change in the shift towards digital technology which now replaces traditional practices.

ADVANCING TECHNOLOGIES FOR THE FUTURE

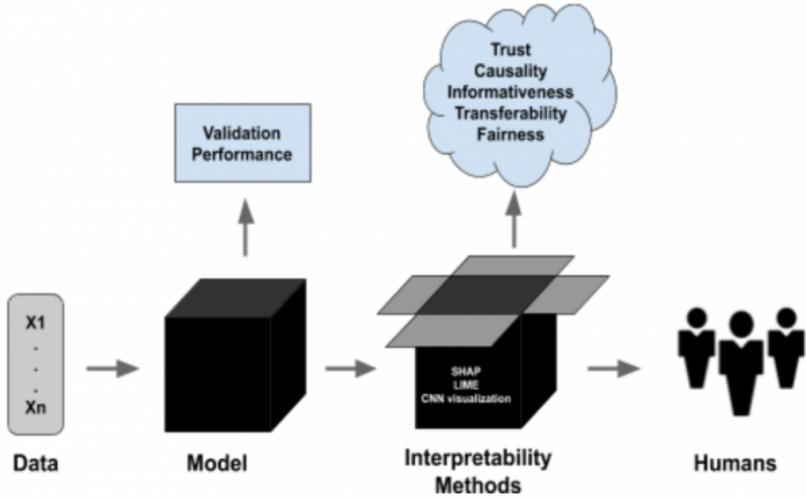
EXPLAINABLE AI: INCREASING TRUST OF AI BLACKBOX

BY MS. SREEJA M U | ASSISTANT PROFESSOR, DIT

Explainable AI (XAI) is an emerging field in machine learning that aims to address how black box decisions of AI systems are made. This area inspects and tries to understand the steps and models involved in making decisions. Unlike generic AI models, where the result of the deployed model is merely a prediction, explainable AI focuses on increasing the trust level of the prediction, overviewing the output of the model to generate inferences which the model has used for deducing the result. Further, the approach aids in deciphering what factors have actually contributed to the results.

In the last few years, AI has achieved a notable success by delivering the best of expectations over many applications. This empirical success of machine learning (ML) and deep learning (DL) models attributes to the combination of efficient learning algorithms and their huge parametric space . The combination of the parametric learning space comprises hundreds of layers and millions of parameters, which makes ML and DL models be considered as complex black-box models. Due to the black-box-ness of the models, AI experts (e.g., engineers and developers) need to search for a direct understanding of the mechanism by which a model works. The transparency, which is the opposite of the black-box-ness

of models, is increasingly being demanded to avoid the danger of making decisions that are not justifiable and do not allow obtaining detailed explanations of their behaviour. For example, in precision medicine, binary predictions are insufficient due to their sensitivity of medicine prescriptions to the patients. Also, for cyber-security, the misleading predictions can make the system vulnerable for attacks and lead to zero-trust security for critical systems.



Use Cases of Explainable AI

Explainable AI finds its use case in domains where technology impacts people's lives fundamentally requiring trust and audibility. These include-

Healthcare: Explainable AI provides a traceable explanation allowing doctors and medical care professionals to trust the outcome predicted by the AI model. Explainable AI acts as a virtual assistant to doctors helping them detect diseases more accurately, for instance, cancer detection through an MRI image identifies suspicious areas as probable for cancer.

Fraud detection: Explainable AI is important for fraud detection in financial services. This can be used to explain why a transaction was flagged as suspicious or legitimate,

which helps mitigate potential ethical challenges associated with unfair bias and discrimination issues when it comes to identifying fraudulent transactions.

Defence: Explainable AI can be useful for military training applications to explain the reasoning behind a decision made by an artificial intelligence system (i.e., autonomous vehicles). This is important because it helps mitigate potential ethical challenges such as why it misidentified an object or did not fire on a target.

Autonomous vehicles: Explainable AI is becoming increasingly important in the automotive industry due to highly publicised events involving accidents caused by autonomous vehicles (such as Uber's fatal crash with a pedestrian). This has placed an emphasis on explainability techniques for AI algorithms, especially when it comes to using cases that involve safety-critical decisions. Explainable AI can be used for autonomous vehicles where explainability provides increased situational awareness in accidents or unexpected situations, which could lead to more responsible technology operation (i.e., preventing crashes).

To conclude, Explainable AI forms a key aspect of ethical AI. Here are the key benefits of using explainable AI:

- Explainable AI is desired in use cases involving accountability. For example, explainable AI could help create autonomous vehicles that are able to explain their decisions in the case of an accident.
- Explainable AI is critical for situations involving fairness and transparency where there are scenarios with sensitive information or data associated with it (i.e., healthcare)
- Enhanced trust between humans and machines
- Higher visibility into model decision-making process (which helps with transparency)

CYBORGS - THE FUTURE MAN KIND

BY ROSNA AUGUSTINE | S7-IT

A cyborg is Part human and part machine(robot), a hybrid of neurons and wires or circuits. It is a human being artificially transformed into a machine by providing a proper interface between man and computer. And Cyborg means “Cyber Organism”. The Society for Neural interfacing (SNI) actively promotes research on innovative approaches dedicated to Neural Interfacing (NIF). Evaluating current technology and its intrinsic limitations it is possible to outline an almost perfect Neural Interfacing technology, however, predictions are largely based on current visions and one's imagination. Thus, the content of this site is expected to be up dated on a regular

TYPES OF CYBORGS :

1 Robot: A cyborg can literally be a robotic form which helps humans with everyday tasks. They can be used for medical purposes, military purposes, or personal use. Service robots assist human's by performing everyday tasks for them, including cleaning, doing laundry, and even cooking. Service robots are programmed to listen to a humans instructions, but those instructions must be precise in order for a service robot to fulfil that task Robots come in many shapes and sizes. Many people believe a robot literally looks like a robot seen above in the picture. However, a computer is a robot. A vacuum is a robot. Robots do something for us, or help us do something with ease.

Robot implications:

1. Cyborg's create an ease of life for the people who own them, which can ultimately cause a dependence on technology deeper than the dependence we already have.

2. Robots and humans may have little distinction between them in the future. "CYBORG: MYTH OR REALITY?" -This article begins discussing the assumptions that cyborgs and humans have little distinction anymore, because people really believe we will rely solely on cyborgs in the future. The author of the article takes a different approach to this assumption by saying that it is not true, because relying on cyborgs goes against values, specifically those embedded in Christianity. Being that a cyborg is a "cybernetically controlled organism", people begin to wonder if they will take over our planet in the future much like the "I, Robot" movie. The article discusses that we have become attached to technology so much that even we are acting like cyborgs. Still, the author does not agree with this, saying that even though cyborgs can be a medical advantage, they still will not take over the human race. While we do have and will have cyborgs, they will not take over and become a necessity for people to live.

3. If robots are used for medical use, will we rely on them more than doctors? "Service Robots: Rise of the Machines (Again)" -This discusses how robotics is taking off to be a multi-billion dollar industry. Currently, the united states are putting in more money than China towards the advancement of service robots. Specifically, money being spent on robots is geared towards a military gain. One robot is being designed to run at cheetah-like speed.

2.Computer and human: We're closer to becoming real cyborgs than most people realise. In the New York Times the other day, there was a great story by Pagan Kennedy about experiments with brain-computer interfaces, which included the stuff you usually hear about, like people moving cursors with their minds. But it also included some new stuff, like Kennedy herself choosing a picture on her phone using just brainwaves — with no drilling into her skull required. And the novel idea of creating a kind of "brain esperanto," or a universal language for people to speak to computers with their minds.

WILL AI TAKE OVER THE WORLD

BY ALIENA ROSE ANTONY | S1 AI&DS

Some of the world's smartest people are scared. Or if not outright scared, then alarmed. The list is long. It includes Bill Gates, Stephen Hawking and so is Elon Musk. They all warn against smart machines, which are so good at doing things due to their advanced artificial intelligence (AI) that they will do bad things to humans. Yes, such events are so far off that it is impossible for us, even the smartest of us, to envision it. Instead, the best we can do is see 50 years down the line, but still a lot of people think that the threat of AI centres on it becoming malevolent rather than benevolent.

Artificial intelligence, just as the name suggests we humans give intelligence to machines so that it can make decisions and even do tasks that humans can do. If we think in another way, we are basically creating humans, or "servants", so that it can do everything humans want without complaining I mean the advantages of having robots are endless since we cannot create them biologically, machines were the way to go. The fact where artificial intelligence becomes dangerous or a threat also lies there. These smart machines or servants, when they resist human control and reaches a stage where it can no longer be controlled, when the intelligence we gave them outpaces us, it becomes dangerous.

Stephen Hawking a physicist that we all admire once said, "Rise of artificial intelligence will either be the best thing that's ever happened to us, or it will be the worst thing. If we're not careful, it very well may be the last thing". Robots when we give it intelligence, it can think just like a human perhaps more, because we humans are pretty clunky and prone to error, we learn through the system of error and trial,

therefore it takes generations to iterate, whereas robots or AI can skip that part of error and trial and the rate at which it can learn new facts are so much faster than humans, and that is where it poses a threat, it can improve upon their own design a lot faster, and soon, they'll probably be able to do so without our help. Hawking says this will create an "intelligence explosion" in which machines could exceed our intelligence and take control. Artificial intelligence holds great opportunity for humanity, encompassing everything from Google's algorithms to self-driving cars to facial recognition software. The AI we have today, however, is still in its primitive stages. Experts worry about what will happen when that intelligence outpaces us. Or, as Hawking puts it, "Whereas the short-term impact of AI depends on who controls it, the long-term impact depends on whether it can be controlled at all." Once humans lose control over robots and AI because of their extreme advancements, the next stage is to take control over humans' "dictatorship", wars, destruction of humankind, a new era of robots or at least that's what the movies say. Movies like the Terminator and Matrix, although they don't tell the direction, in which AI might go down, they all underline the fact, robots take over humans. Another movie that had a totally different perspective on robots and AI was "I, ROBOT", here the robots followed Isaac Asimov's **"Three Laws of Robotics"**,

- 1 – A robot may not injure a human being, or, through inaction, allow a human being to come to harm.
- 2 – A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.
- 3 – A robot must protect its own existence as long as such protection does not conflict with the First or Second Law

invented as a simple, but immutable moral code for robots. The film's plot revolves around an apparent breaking of the laws, when a robot is suspected of murdering a famous scientist. Here the entity (AI) called VIKI controlled the robots, as her artificial intelligence grew, she had determined that

humans were too self-destructive, and created a Zeroth Law, that robots are to protect humanity even if the First or Second Laws are disobeyed. So rather than bringing destruction to humanity it wanted to save humanity from self-destruction by any means even if it involved injuring a certain human. So, we still don't know the outcome of advancing of AI.

Artificial Intelligence is a great tool for development currently. It has revolutionised technology in all industries and solved many problems faced by humanity. But AI is still in its beginning phases and it can also lead to great harm if it is not managed properly. There are many areas in which Artificial Intelligence can pose a danger to human beings and it is best if these dangers are discussed now so that they can be anticipated and managed in the future.

“Unless we learn how to prepare for, and avoid, the potential risks, AI could be the worst event in the history of our civilisation. It brings dangers, like powerful autonomous weapons, or new ways for the few to oppress the many. It could bring great disruption to our economy.” says Stephen Hawking. We still don't know if it possible, at the least most scientists say to develop such advanced technologies it will take many years and what the future has in store for us nobody knows and can't predict because there are so many variables to consider.

CYBER SECURITY

BY RIYA MANOJ | S5 IT

Today, people can send and receive any form of data be it email, audio or video just by the click of a button. But have you ever wondered how securely your data is transmitted without any leakage of information? The answer lies in cybersecurity.

Cyber security is the technique of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. The rapidly changing digital world needs security teams and systems that can adapt to and prepare for unexpected shifts. From the rise of remote and hybrid work to growing cloud migration, cybersecurity leaders must safeguard their enterprises against new attack vectors every day.

Even the most cutting-edge technologies, such as cloud computing, mobile computing, E-commerce, and online banking, require a high level of security. as these technologies store sensitive information about individuals and their security has become a priority. Enhancing cyber security and safeguarding important information infrastructures are critical to the security and economic well-being.

Cyber security tackles three types of threats: Cybercrime, Cyber-attack and cyberterrorism. Cybercrime refers to individuals or groups who attack systems for monetary gain or to cause disruption. Cyber-attack involves politically motivated information gathering. Cyberterrorism is intended to undermine electronic systems to cause panic or fear.

The benefits of implementing and maintaining cybersecurity practices include:

- Business protection against cyberattacks and data breaches.
- Protection for data and networks.
- Prevention of unauthorised user access.
- Improved recovery time after a breach.
- Protection for end users and endpoint devices

Automation has become an integral component to keep companies protected from the growing number and sophistication of cyber threats. Using artificial intelligence (AI) and machine learning in areas with high-volume data streams can help improve cybersecurity in threat detection, threat response and human augmentation.

There is no perfect solution for cybercrimes but we should try our level best to minimise them in order to have a safe and secure future in cyber space.

IMPACT OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING ON TRADING

BY PAUL JOSHI | S5 IT

The use of AI-based methodologies for designing trading systems, both in short-term time frames and for longer-term investing, is gaining traction, and a few companies are actively involved in this subject. However, widespread adoption of this new technology is slow due to a number of problems, the most notable of which is that AI requires the development of new tools and human expertise.

Trading robots have been used in the stock market for a long time. According to a JPMorgan report from 2020, over 60% of trades worth more than \$10 million were completed using algorithms. By 2024, the algorithmic trading market will have grown by \$4 billion, increasing the total volume to \$19 billion. Although it is too early to predict the overall effects of this new technology on the industry, it is almost certain that widespread AI adoption could result in more efficient markets with lower volatility for longer periods of time, with periodic volatility spikes owing to changes in popular algorithms. This is achievable because the impact of human market analysis, as well as the noise associated with it, will be reduced. However, how well this works in practice remains unseen.

The first advantage of Algorithmic Trading is risk reduction in a high-volatility market. The ability to analyse the probable impact of a trade on the market is the second advantage of algorithmic trading. This is particularly important for fund houses and institutional investors who deal with big sums of money and have a visible impact on price changes.

The protection from emotions is the third major benefit of trading algorithms. Traders and investors, like all living things, are subject to emotions such as fear, greed, and losses. These feelings have a negative effect on performance and success. For example, financial markets were already displaying symptoms of oncoming disaster on the eve of the 2008 global financial crisis. The majority, on the other hand, ignored the apparent signs, basking in the euphoria of the bull market that has lasted since the mid-2000s. Algorithms address the issue by guaranteeing that all trades adhere to a set of rules.

There are many great materials on the internet about machine learning, artificial intelligence, and trading. Attempting to tackle a few practical problems is the best way to learn. However, using these tools in trading may be, at least initially, very different for those who are used to drawing lines on charts and following moving averages. They are in most cases ruled out by the mix of skills required to grasp and implement AI.

INTERNET OF THINGS

BY T A LAKSHMI | S3-IT

In recent years, the Internet of Things (IoT) has drawn significant research attention. IoT is considered as a part of the Internet of the future and will comprise billions of intelligent communicating 'things'. The future of the Internet will consist of heterogeneously connected devices that will further extend the borders of the world with physical entities and virtual components. The Internet of Things (IoT) will empower the connected things with new capabilities. Now, let us find out what IoT is.

What is IoT?

The Internet of Things (IoT) describes the network of physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet. These devices range from ordinary household objects to sophisticated industrial tools. With more than 7 billion connected IoT devices today, experts are expecting this number to grow to 10 billion by 2020 and 22 billion by 2025.

What is the history of the Internet of Things?

The idea of adding sensors and intelligence to basic objects was discussed throughout the 1980s and 1990s (and there are arguably some much earlier ancestors), but apart from some early projects including an internet connected vending machine progress was slow simply because the technology wasn't ready. Chips were too big and bulky and there was no way for objects to communicate effectively.

Processors that were cheap and power-frugal enough to be all but disposable were needed before it finally became cost-

effective to connect up billions of devices. The adoption of RFID tags low-power chips that can communicate wirelessly -- solved some of this issue, along with the increasing availability of broadband internet and cellular and wireless networking. The adoption of IPv6 which, among other things, should providing enough IP addresses for every device the world (or indeed this galaxy) is ever likely to need was also a necessary step for the IoT to scale. Kevin Ashton coined the phrase 'Internet of Things' in 1999, although it took at least another decade for the technology to catch up with the vision. "The IoT integrates the interconnectedness of human culture, our 'things' with the interconnectedness of our digital information system 'the internet.' That's the IoT," Ashton told ZDNet.

Adding RFID tags to expensive pieces of equipment to help track their location was one of the first IoT applications. But since then, the cost of adding sensors and an internet connection to objects has continued to fall, and experts predict that this basic functionality could one day cost as little as 10 cents, making it possible to connect nearly everything to the internet.

The IoT was initially most interesting to business and manufacturing, where its application is sometimes known as machine-to-machine (M2M), but the emphasis is now on filling our homes and offices with smart devices, transforming it into something that's relevant to almost everyone. Early suggestions for internet-connected devices included 'blobjects' (objects that blog and record data about themselves to the internet), ubiquitous computing (or 'ubicomputing'), invisible computing, and pervasive computing. However, it was the Internet of Things and IoT that stuck.

Why is the Internet of Things (IoT) so important?

Over the past few years, IoT has become one of the most important technologies of the 21st century. Now that we can connect everyday objects—kitchen appliances, cars, thermostats, baby monitors—to the internet via embedded devices, seamless communication is possible between people, processes, and things.

By means of low-cost computing, the cloud, big data, analytics, and mobile technologies, physical things can share and collect data with minimal human intervention. In this hyperconnected world, digital systems can record, monitor, and adjust each interaction between connected things. The physical world meets the digital world—and they cooperate.

What technologies have made IoT possible?

While the idea of IoT has been in existence for a long time, a collection of recent advances in a number of different technologies has made it practical.

- **Access to low-cost, low-power sensor technology.** Affordable and reliable sensors are making IoT technology possible for more manufacturers.
- **Connectivity.** A host of network protocols for the internet has made it easy to connect sensors to the cloud and to other “things” for efficient data transfer.
- **Cloud computing platforms.** The increase in the availability of cloud platforms enables both businesses and consumers to access the infrastructure they need to scale up without actually having to manage it all.
- **Machine learning and analytics.** With advances in machine learning and analytics, along with access to varied and vast amounts of data stored in the cloud, businesses can gather insights faster and more easily. The emergence of

these allied technologies continues to push the boundaries of IoT and the data produced by IoT also feeds these technologies.

- **Conversational artificial intelligence (AI).** Advances in neural networks have brought natural-language processing (NLP) to IoT devices (such as digital personal assistants Alexa, Cortana, and Siri) and made them appealing, affordable, and viable for home use.

Why Does IoT Matters?

When something is connected to the internet, that means that it can send information or receive information, or both. This ability to send and/or receive information makes things smart, and smarter is better.

Let's use smartphones again as an example. You can listen to any song in the world, but not because your phone has every song stored on it. It's because every song in the world is stored somewhere else (that place is known as "the cloud"), and your phone can request a song, and receive information to stream it.

To be smart, a thing doesn't need to have super storage or a supercomputer inside of it. All a thing has to do is *connect* to super storage or to a supercomputer. Being connected is awesome.

In the Internet of Things, all the things can be put into three categories:

- Sensors that collect information and then send it.
- Computers that receive information and then act on it.
- Things that do both.

And all three of these have enormous benefits that feed on each other.

ARTIFICIAL INTELLIGENCE IN MEDICAL FIELD.

BY PALLAVI AJITH | S1 AI&DS

Artificial intelligence nowadays is right called narrow AI (or weak AI), in that it is planned to accomplish the narrow job (e.g . Only facial recognition or just internet searches or just riding the car). Nevertheless, the long-term goal of some researchers is to produce common AI (AGI or powerful AI). While narrow AI may surpass humans in whatever its particular job is, like playing chess or solving equations, AGI could outperform humans in almost every cognitive work.

Americans get insane beliefs about artificial intelligence (AI) technologies. Ask the average American what they think of AI and they can frequently react with a combination of anxiety, disgust, and fear. However, these very similar AI applications they need to be so nervous about are already benefiting their lives in significant ways.

There may be more acceptability of the inclusion of changing technology at the battlefield in attempts to reach a critical point. Day-to-day engineering may be to be seen as one with artificial intelligence and the justifiable, standard, and reasonable use of military technology to accomplish organizational success. Leading AI specialist, Mr. Andrew Ng sees artificial intelligence as being this current energy, this every device can have no amount without knowledge, but as the devices, we have and rely on today would have no value without electricity.

The primary aim of health-related AI applications is to analyze relationships between prevention or treatment techniques and patient outcomes. AI programs are applied to practices

such as diagnosis processes, treatment protocol development, drug development, personalized medicine, and patient monitoring and care.

AI in medicine is the process of searching large amounts of data to find insights that can improve the quality of care and patient experiences. Its applications are in various stages of development.

Currently, AI is being widely used in medical settings for clinical decision support and medical imaging analysis. These tools help providers make informed decisions about a patient's care. They can also analyze MRIs and other scans to detect lesions or other findings. The challenges that the COVID-19 pandemic created for many health systems also led many healthcare organizations around the world to start field-testing new AI-supported technologies, such as algorithms designed to help monitor patients and AI-powered tools to screen COVID-19 patients.

Unlike humans, AI never needs to sleep. Machine learning models could be used to observe the vital signs of patients receiving critical care and alert clinicians if certain risk factors increase. While medical devices like heart monitors can track vital signs, AI can collect the data from those devices and look for more complex conditions.

According to a report on the Future of Jobs by the World Economic Forum, AI will create 58 million new artificial intelligence jobs by 2022. There is an excellent chance that by 2030 AI will outperform humans in most of the mental tasks but that does not mean it will take away jobs.

ABOUT THE DEPARTMENT

The Department of Information Technology came into existence in the year 2004 after bifurcation of Division of Computing Sciences. The B.Tech. (Information Technology) programme started in the year 2001 under Division of Computing Sciences. The M.Tech programme on Networking Engineering started in the year 2011. Our Programme had been affiliated to the Mahatma Gandhi University, Kottayam, Kerala from the 2001 to the 2014 admissions, and is affiliated to the A.P.J. Abdul Kalam Technological University, Trivandrum, Kerala from the 2015 admissions onwards. The Department imparts training in the area of Computer Networks, Network Security, Software engineering, Mobile Computing, database management systems, Information security, Web designing, Bioinformatics, IoT, Data Mining, Big Data and many ICT related fields. Two new programmes were introduced under the department in the year 2020 and 2021 subsequently.

B.Tech. Artificial Intelligence and Data Science programme introduced in the year 2020 aims at developing the technical skills of students to perform data processing and analysis, which is an essential task in various real-world applications. During the last decade, data science engineering has emerged as one of the most lucrative career fields in technology and allied businesses. This programme aims at building not only the core technologies such as machine learning, deep learning, data modelling and data mining, but also gives intensive inputs in the evolution of technology.

To address the growing need of engineering talent with skills in digital technology, Rajagiri School of Engineering & Technology in partnership with India's leading Information Technology (IT) Service and Consulting Company – TCS has introduced a new BTech programme in the year 2021 named 'Computer Science & Business Systems' (CSBS) under Department of IT.