Futuristic Features Coming Soon To Smartphones

Contents:-

1. *Photonic Crystal Displays*
2. *Nano-Tech Batteries*
3. *Liquid Buttons*
4. *Headphone Surround Sound*
5. *Biometric Authentication*
6. *Virtual Reality*
7. *Graphene*
8. *No SIM Cards*
9. *Pressure-Sensitive Screens*
10. *Flawless Voice Interaction*
11. *Innovative Medical Apps*
12. *Smart Cameras*

1. Photonic Crystal Displays

While most current smartphone screens are capable of displaying a wide range of incredibly saturated colors, most of them don't adapt too well to varying light conditions. Research and development is now pointing to photonic crystals as the answer to this limitation.

Instead of giving off bright light like LCD or OLED displays, a photonic crystal display features nanostructures that adapt and modify themselves according to the amount of ambient light in a given environment. Although the photonic screen requires an external light source in order to be visible, this could easily be integrated into the body of the phone just like it is in e-readers like the Kindle Paper white.Samsung had already demonstrated the concept of a flexible phone that utilized a photonic crystal display. Chances are we'll start seeing these displays put into smartphones within the next few years.

2. Nano-Tech Batteries

In 2015, at the Mobile World Congress event, Israeli tech company StoreDot revealed a customized Samsung Galaxy S5 with a nano technology-utilizing battery that could charge from 0 to 100 percent in less than a minute.

The technology evolved out of research being conducted in the treatment of Alzheimer's disease. Through their study, scientists learned that peptide molecules, which are responsible for the disease, have an incredibly high capacitance—making them excellent little electrical storage units. The only catch is that, in its current state of development, the StoreDot battery only lasts about two-thirds of the time of a conventional lithium-ion smartphone battery. However, it shouldn’t take too long for the company to improve the technology. StoreDot has already received substantial investments from Samsung, and is in discussions with manufacturers about integrating its battery into future smartphones.

3. Liquid Buttons

Years ago it was the norm that most phones had physical keyboards and any mobile device without one seemed “out of touch.” But currently the opposite is true, and most people think that tactile keyboards look old-fashioned. Well, that’s all set to change again thanks to Tactus Technology and their development of a keyboard that looks like it came from some sort of advanced alien civilization.The keyboard uses special microfluidics technology which drives small amounts of liquid into invisible pockets that rest over the typing pad on a smartphone. When the user brings up the touchscreen keyboard, the pockets instantly fill with liquid which has the effect of physically raising the buttons. The technology has already been incorporated into a new Phorm case for the iPad Mini, but it wouldn’t be too much of a stretch to see it directly built in to future smartphones and tablets.

4. Headphone Surround Sound

Surround sound on headphones has been met with some pretty harsh assessments in the past, but now audio developer DTS is looking to silence the critics with a 7.1 mobile audio solution for smartphones that promises to faithfully recreate the sound of specific listening environments using even the simplest pair of headphones. Though there’s a little ways to go before the system works with all source material, the higher processing power of new smartphones should be able to support the advancement in audio technology.

5. Biometric Authentication

Though the iPhone 6 and the Samsung Galaxy S6 both use capacitive technology to read the ridges of your finger tips, this technology could be considered lacking from a security perspective because it doesn’t use enough data points, which makes it more susceptible to being hacked. Improving on the concept, telecommunications company Qualcomm has developed a new type of ultrasonic fingerprint scanner using a piezoelectric layer that creates ultrasound. In addition to mapping your finger, the scanner features greatly increased resolution, which is also an enhanced security benefit.

6. Virtual Reality

With soon-to-be-released headsets like Oculus Rift, Playstation VR and HTC Vive stealing all the virtual reality-related headlines, not much attention has been given to the VR technology on smartphones. Nonetheless, the new 4K displays that will be rolling out on new smartphones in 2016 are ideal for VR applications.

Once inserted into a head-mounted device, the phone itself will act as the VR headset's display and 4K resolution will be instrumental in providing an immersive, non-pixellated experience. Of course, this may or may not be a good thing considering a lot of us already bury our faces in our phones and ignore what's going on in the world around us.

7. Graphene

Since its development for practical application in 2004, graphene has been praised as "wonder material" by nearly everyone in the electronics industry. It's thin, lightweight, flexible, transparent and over 200 times stronger than steel. It's also one of the best materials for conducting electricity, which makes it ideal for use in electronic devices.

Incorporating graphene into smartphones could allow for designs to be ultra-thin, transparent, flexible and virtually indestructible. Recently, there have been a few breakthroughs by phone manufacturers who have been playing around with graphene. Most notably, Samsung's Advanced Institute of Technology (SAIT) produced graphene in a way that allowed it to retain its outstanding electrical qualities—a problem that had proved to be a serious challenge up to that point. This development should make flexible, transparent smartphone displays commercially viable within the next couple of years.

8. No SIM Cards

Although manufacturers have made efforts to reduce the size of SIM cards, they still feel very much like a leftover relic of the '90s. Thankfully, Apple and Samsung are making strides to rid the world of the physical presence of SIM cards by replacing them with an electronic version.

By having a programmable SIM integrated into your phone, you'll essentially be able to switch between network providers at the drop of a hat without having to request a new SIM card. Which should come in quite handy for anyone travelling or living abroad who wants to get set up with a local number. It's said that the technology could be available in new smartphones as early as next year.

9. Pressure-Sensitive Screens

The Force Touch on the Apple Watch has demonstrated that companies already have the ability to manufacture screens that are capable of sensing pressure. Controls that can distinguish between a light tap from a firm press will give users even more ways to manipulate their phones and has obvious benefits for the gaming community.

In addition to Apple, Samsung has filed a patent for something called "Touch Display Apparatus Sensing Force," which clearly uses the same technology, and in July 2015, Chinese manufacturer ZTE revealed the ZTE Axon Mini which also features a pressure-sensitive touch screen.

10. Flawless Voice Interaction

Voice interaction has been around for a while now and incremental improvements over the years have led to the development of virtual personal assistants and knowledge navigators like Apple's Siri. But that's just the tip of the iceberg. The algorithms used in voice-assisted applications are moving ahead at break-neck speed. With the technology improving so quickly, it won't be long before the A.I. becomes so intuitive that it will start giving you advice that seems to pre-empt your very thoughts. Let's just hope that the developers remember to program Asimov's three laws of robotics into them so we don't wind up subservient to our smartphones in the future.

11. Innovative Medical Apps

Recently, scientists developed an app called Athelas which makes use of a lens attachment to track malaria and cancerous cells as they move through a patient's blood. This innovation has prompted scientists to look for other ways that smartphones could be used to track highly infectious diseases, such as Ebola, to gain a better understanding of how they move and spread.Using an inexpensive phone add-on called PCR that's able to tag and track pathogens in the blood, diseases should be able to be diagnosed within hours or even minutes. The data gathered would then be automatically uploaded from the phone to an online database where other scientists can analyze it.When you combine this emerging technology with other existing applications that are able to track things like blood-pressure and heart rate, it's easy to see how smartphones could soon bring about a revolution in medical care.

12. Smart Cameras

This technology could have enormous potential and enable cameras to do all sorts of clever and useful things relating to the real world environment. Google has also been developing a similar type of deep search identification software with Google Photos. As camera hardware continues to shrink and improve, it seems inevitable that this sort of feature will become standard on phones.

F/No. 105021247
HC/RO PRADEEP GUPTA

Cyber-security

What is cybersecurity?

Cybersecurity is the practice of protecting internet-connected systems such as hardware, software and data from cyberthreats. It's used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

An effective cybersecurity strategy can provide a strong security posture against malicious attacks designed to access, alter, delete, destroy or extort an organization's or user's systems and sensitive data. Cybersecurity is also instrumental in preventing attacks designed to disable or disrupt a system's or device's operations.

An ideal cybersecurity approach should have multiple layers of protection across any potential access point or attack surface. This includes a protective layer for data, software, hardware and connected networks. In addition, all employees within an organization who have access to any of these endpoints should be trained on the proper compliance and security processes. Organizations also use tools such as unified threat management systems as another layer of protection against threats. These tools can detect, isolate and remediate potential threats and notify users if additional action is needed.

Cyberattacks can disrupt or immobilize their victims through various means, so creating a strong cybersecurity strategy is an integral part of any organization. Organizations should also have a disaster recovery plan in place so they can quickly recover in the event of a successful cyberattack.

Why is cybersecurity important?

With the number of users, devices and programs in the modern enterprise increasing along with the amount of data -- much of which is sensitive or confidential -- cybersecurity is more important than ever. But the volume and sophistication of cyber attackers and attack techniques compound the problem even further.Without a proper cybersecurity strategy in place -- and staff properly trained on security best practices -- malicious actors can bring an organization's operations to a screeching halt.

What are the elements of cybersecurity and how does it work?

The cybersecurity field can be broken down into several different sections, the coordination of which within the organization is crucial to the success of a cybersecurity program. These sections include the following:

- Application security.
- Information or data security.
- Network security.
- Disaster recovery and business continuity planning.
- Operational security.
- Cloud security.
- Critical infrastructure security.
- Physical security.
- End-user education.

Maintaining cybersecurity in a constantly evolving threat landscape is a challenge for all organizations. Traditional reactive approaches, in which resources were put toward protecting systems against the biggest known threats while lesser-known threats were undefended, are no longer a sufficient tactic. To keep up with changing security risks, a more proactive and adaptive approach is necessary. Several key cybersecurity advisory organizations offer guidance. For example, the National Institute of Standards and Technology (NIST) recommends adopting continuous monitoring and real-time assessments as part of a risk assessment framework to defend against known and unknown threats.

What are the benefits of cybersecurity?

The benefits of implementing and maintaining cybersecurity practices include the following:

- Business protection against cyberattacks and data breaches.
- Protection of data and networks.

- Prevention of unauthorized user access.
- Improved recovery time after a breach.
- Protection for end users and endpoint devices.
- Regulatory compliance.
- Business continuity.
- Improved confidence in the company's reputation and trust for developers, partners, customers, stakeholders and employees.

What are the different types of cybersecurity threats?

Keeping up with new technologies, security trends and threat intelligence is a challenging task. It's necessary in order to protect information and other assets from cyberthreats, which take many forms. Types of cyberthreats include the following:

- *Malware* is a form of malicious software in which any file or program can be used to harm a user's computer. Different types of malware include worms, viruses, Trojans and spyware

  .
- *Ransomware* is a type of malware that involves an attacker locking the victim's computer system files -- typically through encryption -- and demanding a payment to decrypt and unlock them.
- *Social engineering* is an attack that relies on human interaction. It tricks users into breaking security procedures to gain sensitive information that's typically protected.
- *Phishing* is a form of social engineering in which fraudulent email or text messages that resemble those from reputable or known sources are sent. Often random attacks, the intent of phishing messages is to steal sensitive data, such as credit card or login information.
- *Spear phishing* is a type of phishing that has an intended target user, organization or business.
- *Insider threats* are security breaches or losses caused by humans -- for example, employees, contractors or customers. Insider threats can be malicious or negligent in nature.

- *Distributed denial-of-service (DDoS) attacks* are those in which multiple systems disrupt the traffic of a targeted system, such as a server, website or other network resource. By flooding the target with messages, connection requests or packets, DDoS attacks can slow the system or crash it, preventing legitimate traffic from using it.

- *Advanced persistent threats (APT)* is a prolonged targeted attack in which an attacker infiltrates a network and remains undetected for long periods of time. The goal of an APT is to steal data.

- *Man-in-the-middle (MitM)) attacks* are eavesdropping attacks that involve an attacker intercepting and relaying messages between two parties who believe they're communicating with each other.

- *SQL injection* is a technique that attackers use to gain access to a web application database by adding a string of malicious SQL code to a database query. A SQL injection provides access to sensitive data and enables the attackers to execute malicious SQL statements.

Other common types of attacks include botnets, drive-by-download attacks, exploit kits, malvertising, vishing, credential stuffing attacks, cross-site scripting attacks, keyloggers, worms and zero-day exploits.

Cybersecurity best practices

To minimize the chance of a cyberattack, it's important to implement and follow a set of best practices that includes the following:

- *Keep software up to date*. Be sure to keep all software, including antivirus software, up to date. This ensures attackers can't take advantage of known vulnerabilities that software companies have already patched.

- *Change default usernames and passwords.* Malicious actors might be able to easily guess default usernames and passwords on factory preset devices to gain access to a network.

- *Use strong passwords.* Employees should select passwords that use a combination of letters, numbers and symbols that will be difficult to hack using a brute-force attack or guessing. Employees should also change their passwords often.

- *Use multifactor authentication (MFA).* MFA requires at least two identity components to gain access, which minimizes the chances of a malicious actor gaining access to a device or system.

- *Train employees on proper security awareness.* This helps employees properly understand how seemingly harmless actions could leave a system vulnerable to attack. This should also include training on how to spot suspicious emails to avoid phishing attacks.
- *Implement an identity and access management system (IAM).* IAM defines the roles and access privileges for each user in an organization, as well as the conditions under which they can access certain data.
- *Implement an attack surface management system.* This process encompasses the continuous discovery, inventory, classification and monitoring of an organization's IT infrastructure. It ensures security covers all potentially exposed IT assets accessible from within an organization.
- *Use a firewall.* Firewalls restrict unnecessary outbound traffic, which helps prevent access to potentially malicious content.
- *Implement a disaster recovery process*. In the event of a successful cyberattack, a disaster recovery plan helps an organization maintain operations and restore mission-critical data.

How is automation used in cybersecurity?

Automation has become an integral component to keeping companies protected from the increasing number and sophistication of cyberthreats. Using artificial intelligence (AI) and machine learning in areas with high-volume data streams can help improve cybersecurity in the following three main categories:

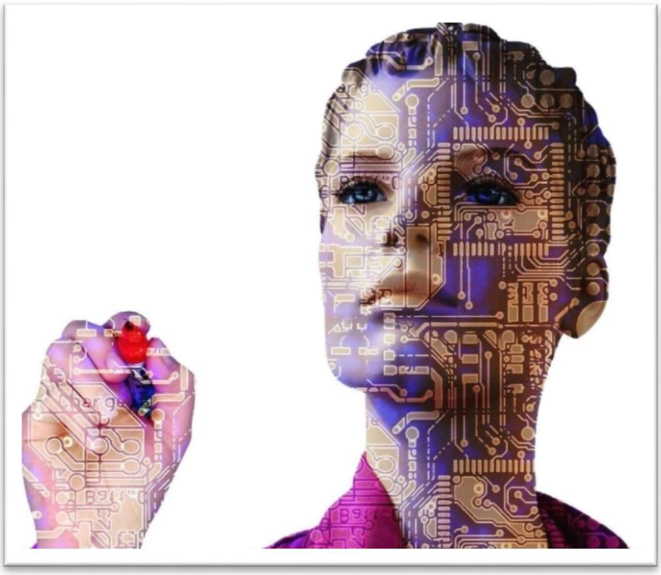
- *Threat detection.* AI platforms can analyze data and recognize known threats, as well as predict novel threats that use newly discovered attack techniques that bypass traditional security.
- *Threat response*. AI platforms create and automatically enact security protections.
- *Human augmentation.* Security pros are often overloaded with alerts and repetitive tasks. AI can help eliminate alert fatigue by automatically triaging low-risk alarms and automating big data analysis and other repetitive tasks, freeing humans for more sophisticated tasks.

F/No. 041568065
ASI/T SANEESH S

A Brief Introduction to Artificial Intelligence

What is AI and how is it going to shape the future

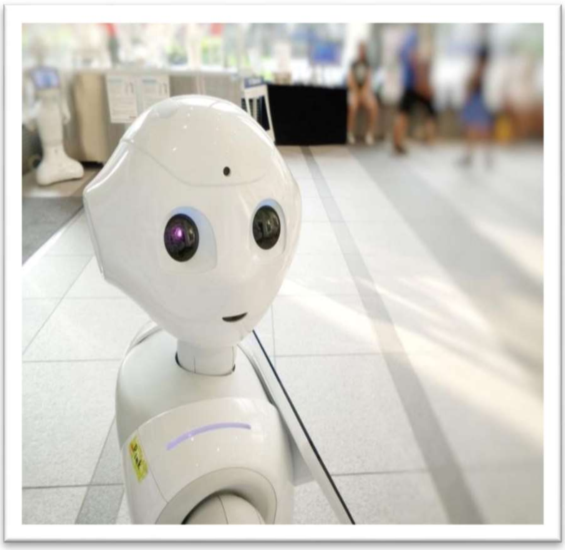
What is Artificial Intelligence?



Generally speaking, Artificial Intelligence is a computing concept that helps a machine think and solve complex problems as we humans do with our intelligence. For example, we perform a task, make mistakes and learn from our mistakes (At least the wise ones of us do!). Likewise, an AI or Artificial Intelligence is supposed to work on a problem, make some mistakes in solving the problem and learn from the problems in a self-correcting manner as a part of its self-improvement. Or in other words, think of this like playing a game of chess. Every bad move you make reduces your chances of winning the game. So, every time you lose against your friend, you try remembering the moves you made which you shouldn't have and apply that knowledge in your next game and so on. Eventually, you get better and your precision, or in this case probability of winning or solving a problem

improves by a noteworthy extent. AI is programmed to do something similar to that!

Artificial Intelligence vs Traditional Robotics



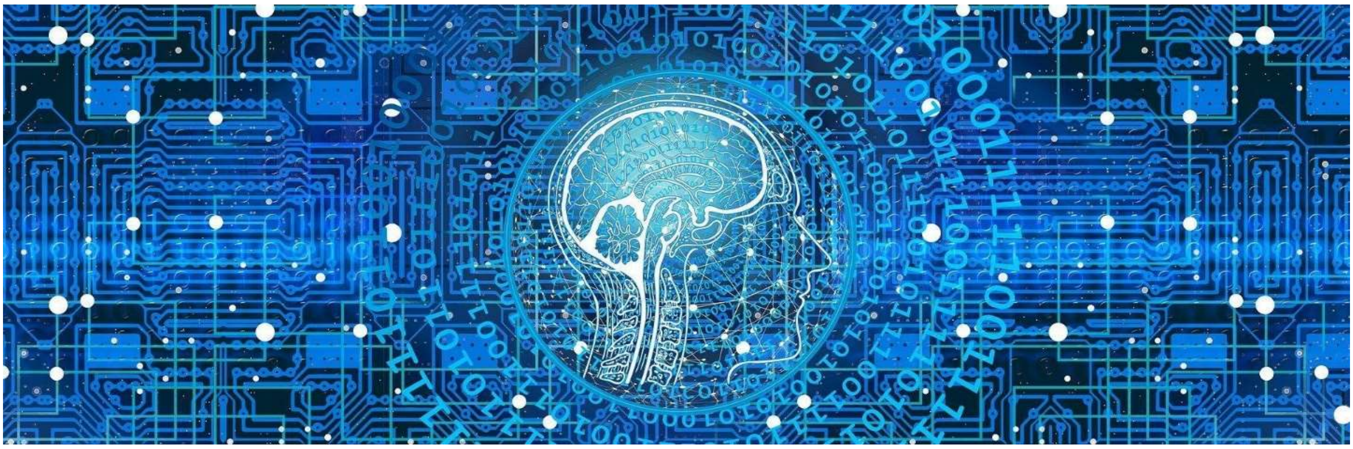
When we hear the word "Robot", an image of a metal box with creepy eyes and speaking in a mechanical voice pops into our head. I mean that's what we have been watching in television for years, isn't it? And to a certain degree we are right. Traditional robotics has been perceived by pop culture as an arena that creates humanlike machines to work for us as saviours and sometimes as super-villains bringing in a cascade of tyranny into the human world. However, real life robots aren't as humanlike as we want them to be, yet. They are programmed in a specific way to only execute tasks that it has been programmed to perform.

Imagine a self-driving car that has been designed to drive you on its own according to where you instruct it to take you. Now for a traditional robot, the car is going to go through the exact road that it was programmed to select for a certain destination by its creators, possibly without the knowledge of traffic and cause accidents. However, a human driver would have chosen the shortest path or check which paths have the least traffic today and would be the most convenient path for that particular destination. That is the exact humanlike creative thinking the traditional robots lack! They are fixed in their own "not so smart" way and are largely dependent on the program they are built on and the instructions that they are being given. If a certain instruction doesn't coincide with their program, the robot won't even be able to run, let alone going the extra step of being creative. This is the limitation of traditional robots Artificial Intelligence is being developed to overcome. Unlike the conventional "bips and bops", a good AI will simulate the complicated and intuitive sense of thinking and problem-solving abilities of the human mind.

A Brief History of AI

The concept of Artificial Intelligence is not as modern as we think it is. This traces back to as early as 1950 when Alan Turing invented the Turing test. Then the first chatbot computer program, ELIZA, was created in the 1960s. IBM deep blue was a chess computer made in 1977 beat a world chess champion in two out of six games, one won by the champion and the other three games were draw. In 2011, Siri was announced as a digital assistant by Apple. Elon Musk and some others founded OpenAI in 2015.

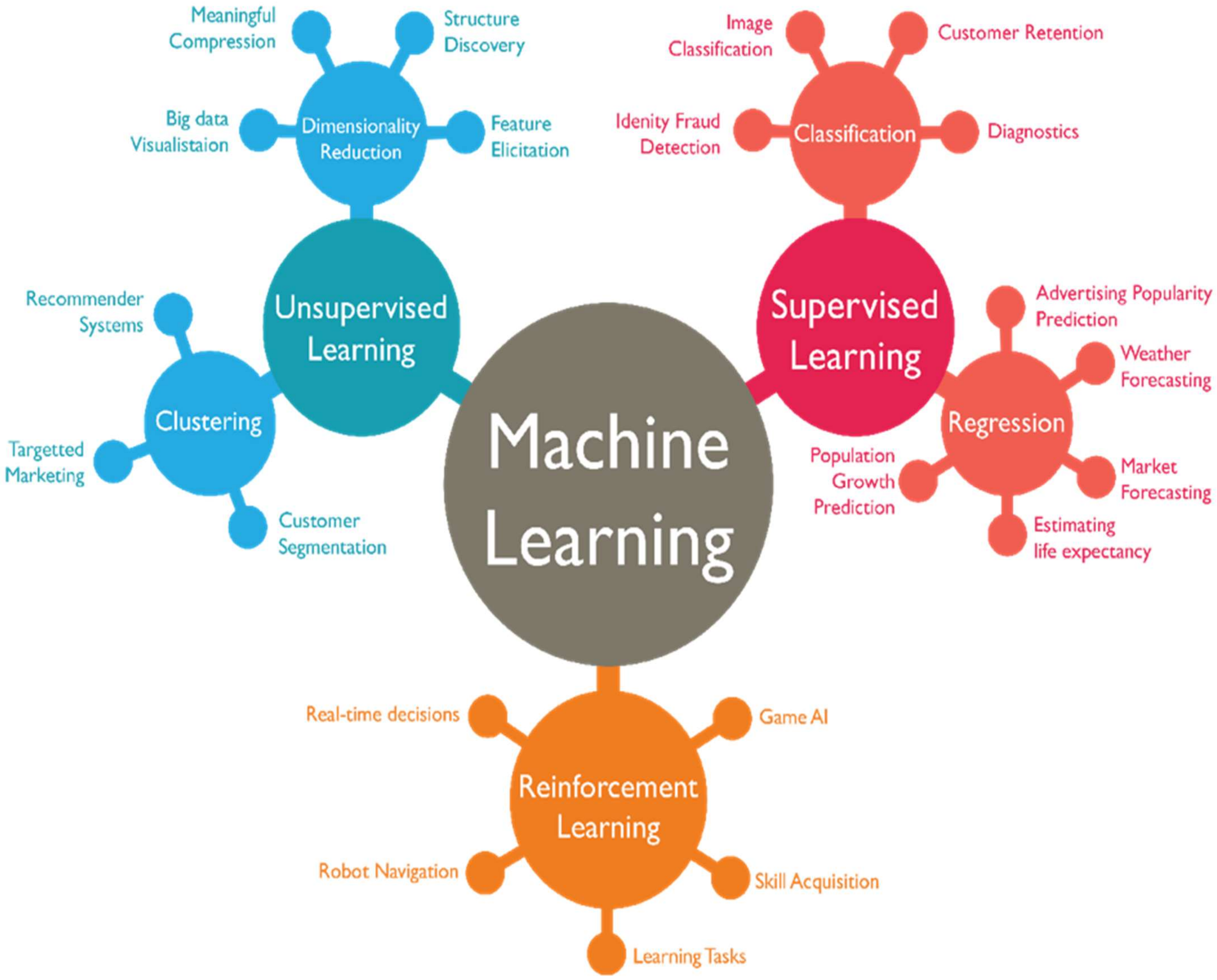
Artificial Intelligence vs Machine Learning vs Deep Learning



Artificial Intelligence as a process that is going to help machines achieve a humanlike mental behavior. AI is a vast and growing field which also includes a lot more subfields like machine learning and deep learning and so on. Machine learning is in a nutshell the concept of computers learning to improve their predictions and creativity to resemble a humanlike thinking process using algorithms. Machine learning involves a number of learning processes such as:

Supervised learning: Supervised learning is a process where our machines are designed to learn with the feeding of labelled data. In this process our machine is being trained by giving it access to a huge amount of data and training the machine to analyze it. For instance, the machine is given a number of images of dogs taken from many different angles with colour variations, breeds and many more diversity. So that, the machine learns to analyze data from these diverse images of dogs and the “insight” of machines keep increasing and soon the machine can predict if it’s a dog from a whole different picture which was not even a part of the labelled data set of dog images the machine was fed earlier.

Unsupervised learning: Contrary to the supervised learning, the unsupervised learning algorithms comprises analyzing unlabelled data i.e., in this case we are training the machine to analyze and learn from a series of data, the meaning of which is not apparently comprehendible



by the human eyes. The machine looks for patterns and draws conclusions on its own from the patterns of the data. Important thing to remember that the dataset used in this instance is not labelled and the conclusions are drawn by the machines.

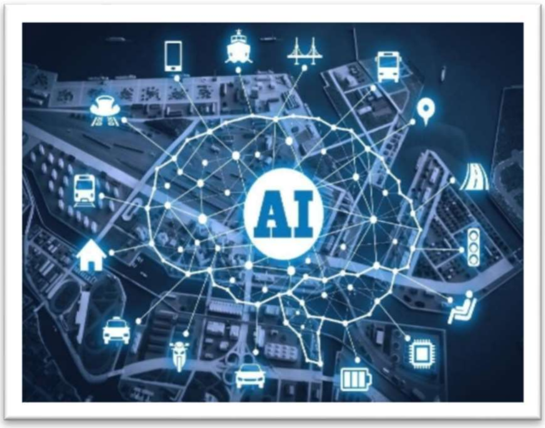
Reinforcement learning: Reinforcement learning is a feedback dependent machine learning model. In this process the machine is given a data and made to predict what the data was. If the machine generates an inaccurate conclusion about the input data, the machine is given feedback about its incorrectness. For example, if you give the machine an image of a basketball and it identifies the basketball as a tennis ball or something else, you give a negative feedback to the machine and eventually the machine learns to identify an image of a basketball on its own when it comes across a completely different picture of a basketball.

Deep Learning, on the other hand is the concept of computers simulating the process a human brain takes to analyze, think and learn. The deep learning process involves something called a neural network as a part of the thinking process for an AI. It takes an enormous amount of data to train deep learning and a considerably powerful computing device for such computation methods.

AI at Work Today

The most common examples of uses of Artificial Intelligence can be found today in smart personal assistants like Apple's Siri and Amazon's Alexa. People interact with these devices to command them on a daily basis and these devices use the commands as a part of their dataset to learn from. Another known example of Artificial Intelligence is the use of algorithms in Netflix. Netflix provides very much accurate and relevant suggestions of movies, tv series from our data which is created every time we stream or click on something in Netflix. As the dataset for these systems grows, their accuracy and precision increase as well. Artificial Intelligence is also viewed as a great tool for better cybersecurity. Many banks are using AI as a means to identify unauthorized credit cards uses. From analyzing complex genetic data to perform the most delicate surgeries at the highest precision is also being worked on to integrate with AI. We all know about companies like Tesla and Apple working to make flawless self-driving cars which is going to have game changing impacts on the future of transportation.

Artificial Intelligence and The Future



It is said that AI is the greatest thing humankind has ever worked on. AI is being used in image and speech recognition and analysis which will be far better than human recognition of image and speech and its application stretches wide and far. There are research and works being conducted using AI that is going to play a very important role in our future healthcare. AI is being worked on to cure Alzheimer's disease and someday even blindness. Someone with dyslexia is being helped to read better with the help of AI. Genetic data is being analyzed by bioinformatics; data science integrated with AI for way better data analysis in healthcare that has not been possible for us in the past. Fields like cancer research and other such diseases are being impacted greatly by advanced applications of AI. AI can be a great tool in the future of education. AI can be used to analyze data from an individual's personal and intellectual needs, capabilities, choices and limitations to develop customized curriculum, strategies and schedules that will be more well suited, appealing and inclusive of most, if not all, children and adults. The uses of AI are also going to change the way we are going to commute in the future. In addition to self-driving cars, work is being done to manufacture "self-flying" planes and drones that conveniently deliver your food faster and better. One of the biggest concerns about AI is that jobs are being replaced due to automation. However, AI might be creating more jobs than it replaces. This will change the way humans work by creating new types of jobs.

AI is still in a fairly preliminary (but rapidly growing) stage today and it requires more and more training to develop. Trainers, engineers, system designers and software developer jobs in machine learning, data science and many such related fields are being created in abundance. New business and investment opportunities are also on the rise due to endless AI applications in agriculture, education, transportation, finance, biotechnology, cybersecurity, gaming etc. As new businesses are being created so are new jobs. Many existing jobs are becoming redefined and more specialised which is really important for the new world to prosper and advance.

Towards Conclusion…

The growth of Artificial Intelligence in recent times has been exponential. We cannot even imagine how big and impactful AI is going to be in the near future and how drastically it is going to change and upgrade the world we live in today. There are a lot more to learn about AI and its rapidly growing applications in our life. I believe it would be wise to adapt to this changing world and acquire skills related to Artificial Intelligence and technology. Just like AI learns and develops, we should too - to make this world a better place.

F/No. 841030294
SI/RF AJOY KR MISHRA

Information Technology ACT & Cyber Crime

- ***INTRODUCTION:***

Internet has become the most significant technology all over the world, which is not only used by the people to contact each other but also utilized by business organizations to become global. Computer and internet enable business organizations to execute the Electronic commerce business model, which has become very popular. Computers and Internet are a powerful source in the success of globalization and international business. Computers are being used worldwide and cybercrime is a global issue plaguing the world. Cybercrime has become an important concern for not only the business firms, government, law enforcement agencies but also for the common people because these kinds of issues are related to the consumer's day-to-day activities. Due to these types of crimes, consumer's money, business organization's integrity, consumer and company's privacy, etc. are in danger.

- ***CYBER CRIME :***

There is no single definition of cybercrime but it can be generally termed as any unlawful or criminal activity done with the help of computer system, communication devices, Internet, Network, Cyberspace and web. There are crimes that are only committed on the Internet and are created exclusively because of the World Wide Web. Now-a-days, Cloud computing has become more popular among the people and Corporates which concentrates and encompasses more and more sensitive data. Inadequate security makes it susceptible to cyber criminals. Cybercrime includes hacking, Data Diddling, Data Theft, Cyber Stalking, Cyber terrorism, email spoofing, Email Spamming, Email Bombing, Terrorism funding, Online fraud, Phishing/ wishing, Web defacement, Denial of service, Virus and worms, pornography, software piracy, digital signature, etc.

- ***SOURCE OF ATTACK :***

Insiders: Current employees, former employees, Current service providers/consultants/ contractors, former service providers/ consultants/contractors, Suppliers, Business partners and customers Outsiders: Terrorists organized Crime, competitors, Information broker, activists/hackers, foreign states/entities and many others.

- ## ***CATEGORIES OF CYBER CRIMES:***

i) Data diddling:

Data diddling involves changing data prior or during input into a computer. In other words, the data is not entered in the system in the way it should have been entered. Section 43(d) read with section 66 of IT Act, which prescribes a punishment of imprisonment which may extend to three years or fine up to Rupees five lakhs or both.

ii) Data Theft:

Data Theft means stealing company data and this can be done through USB, E-mail, Etc. Data Theft also includes copying or stealing the web pages of the company. Data Theft Protection tool: Falconstor Continues data protector, McAfee Data Loss Prevention, PKware partner Link, RSA Data Loss Prevention Suite, Websense's Content Protection Suite, etc. A person can be prosecuted under Section 43(b) of IT Act read with section 66. The penalty is fine which may extend to Rs. five Lakhs or imprisonment which may extend to three years or both.

iii) Cyber Stalking:

Constantly sending messages to harass the recipient emotionally. No provision in IT Act but prosecution under Indian Penal Code is possible.

iv) Cyber Terrorism:

It is an activity of potentially attacking large number of people by cheaper methods than traditional. It is act of doing real world crime using cyberspace. Section 66F of IT Act prescribes a punishment of imprisonment which may extend for Life.

v) Email Spoofing:

Here the e-mail will appear to have been sent from one source but actually it will be sent from another source. Section 66D of IT Act prescribes the punishment for this offence which may extend to three years of imprisonment.

vi) Other Categories:

Other category includes, Email Spamming, Email Bombing, Phishing/vishing, Unauthorized Access & Hacking, Virus, Website Defacement, Denial of services, Pornography/pedophiles, etc.S

- ## ***CYBER SECURITY :***

Cyber security comprises technologies, processes and controls that are designed to protect systems, networks and data from cyber-attacks.
Effective cyber security reduces the risk of cyber-attacks, and protects organizations and individuals from the unauthorized exploitation of systems, networks and technologies.

- ***Consequences of absence of cyber security:***

i) Data/Information may get destroyed, stolen or exposed

ii) System availability may be denied or degraded

iii) Present or former employees or customers may get personally impacted

iv) Lawsuits

v) Damage to Corporate/Brand Image Security Measures

vi) Don’t leave the unencrypted data (words, images, reports, etc.) in the email boxes

vii) Complying with requirement of laws (HIPAA, SOX, etc.) is not enough to secure your data; it is equally important to follow standards issued by various International bodies like ISACA, ISO, ICAI, IIA, etc.)

viii) Security Assessment and building a roadmap with the help of standards like ISO 27001

ix) Involvement of Top level management (BOD) and availability of enough financial resources

x) Review and update of Security policies, procedures and supporting resources

xi) Design and regular testing of business continuity plans and disaster recovery plans

- ***CASES WHICH CAN BE REGISTERED UNDER IPC:***

Offences by/against Public Servant (Sections 167, 172, 173, 175) False electronic evidence(Section 193) Destruction of electronic evidence (Sections 204, 477) Forgery (Sections 463, 465,466, 468, 469, 471, 474, 476, 477A) Criminal Breach of Trust (Sections 405, 406, 408, 409)Counterfeiting Property Mark (Sections 482, 183, 483, 484, 485) Tampering (Section 489) Counterfeiting Currency/Stamps (Sections 489A to 489E).

- ***THE CONCLUSION :***

It can be seen that the threat of computer crime is not as big as the authority claim. There will always be new and unexpected challenges to stay ahead of cyber criminals and cyber terrorists but we can win only through partnership and collaboration of both individuals and Government. There is much we can do to ensure a safe, secure and trustworthy computing environment. It is crucial not only to our national sense of well-being, but also to our national security and economy.

F/No. 085206352
HC/RO PRABHAT KUMAR

Acknowledgement

We are highly thankful for reading out this compilation and hope it will be useful for you in day to day professional and personal life. We would like to hear your interest areas, suggestions from you to make this newsletter more informative and interesting. Your views will definitely help us to create this newsletter as an effective medium to reach you with latest development in the fields of communication and technology.

R&D Team

CTC T&IT CRPF, Ranchi, Jharkhand

ctcit@crpf.gov.in