

The Applications of Artificial Intelligence and Machine Learning

Posted on January 6, 2024

Abstract

The applications of [artificial intelligence](#) and machine learning under the umbrella of computer science and its diverse fields have become popular as both disciplines are interdependent and used interchangeably in science. This work aims to clarify the symbiotic relationship used interchangeably between machine learning and artificial intelligence, different types of learning in AI-assisted systems, biases and their mitigations, applications of software assurance in AI-based systems, and contributions of AI in the world. The present study seeks to provide more theoretical and terminological clarity into the role of ML and AI in building agents that mimic human intelligence in an efficient and intelligent manner. In today's ever-emerging era of technology, neural networks are the hottest area of AI and ML that deals with natural language processing, voice and text recognition, and image processing. Therefore, neural networks are contributing the most in the area of AI languages that work effectively with maximum potential to decrease human effort, replacing it with intelligent agents and AI-based machines.

What is Artificial Intelligence (AI)?

At some point in our daily lives, most of us use Cortana, Siri, Bixby, or even Google Assistant, which helps us find useful information through the use of our voice. We can ask, "Hey Siri, can you please find me the closest coffee shop?" or "Hey Google, can you please play a song from the album "Narrated For You" by Alec Benjamin as I am feeling a bit sad?" and Google plays it for you. However, the question arises as to how this software works and what is significance in today's ever-emerging world of technology. The answer is that they are our personal digital assistants that help us find useful information over the technology of the internet when we ask for it. They respond to our queries with relevant information by either searching the millions of websites or going through the minute options and applications installed on our phones. This is the simplest example of AI and its usage in the world. However, we take this term for granted and do not phrase a formal definition of what this holistic term means and implies in our daily lives. Traditionally, AI is a branch of Computer Science, but its definitions have shifted across a wide spectrum from many areas of academic arenas to business and technology that utilize a range of definitions depending on the objectives and background of the fields. The reason why the field of AI is difficult to define is that different definitions are derived from multiple paradigms and are often dependent on context. The first paradigm is human performance-centered, and the other depends on the reasoning power as well as thought processes where man

and machine try to “outthink” each other where it is difficult to think and tell where the machine begins and man ends.

Evolving Definitions of Artificial Intelligence

As with any concept, it is presently difficult to define the discipline of AI in a detailed and generally accepted form; there are certain definitions combed through different reputable and authentic resources depending on the different information asked and according to different paradigms. The introductory definition of AI is meant to reflect the discipline of engineering and science for making smart and intelligent machines, advanced computer systems in particular, to understand human intelligence. Although these advanced machines mimic human intelligence, the field does not confine itself to the biologically observable method (McCarthy, 2004). It is commonly deliberated that AI came as a subject/discipline at a conference where a system Logic Theorist was demonstrated as proof to theorems in symbolic logic by Herb Simon and Alan Newell. The conference “The Dartmouth Summer Research Project on Artificial Intelligence,” organized by Marvin Minsky and John McCarthy, introduced many other systems along with Logic Theorist that was the “first foray by AI into high-order intellectual processes” (McCarthy et al., 2006). Other systems, including Dendral and Mycin mechanized organic chemistry and its impacts, are found in scientific reasoning and also diagnosed infectious diseases, respectively. This initial success led to the hypothesis proposed by Simon and Newel in 1976 that is known as the “Physical Symbol Systems Hypothesis” As Simon and Newel stated, “a physical symbol system has the necessary and sufficient means for general intelligent actions” (Newell & Simon, 2007).

Today, modern-day definitions of AI consider it a sub-field of computer science that implies how advanced machines can imitate human intelligence in a smart and intelligent way. In another paradigm, AI is “the theory and development of computer systems that are able to perform tasks normally requiring human intelligence such as decision making, perception, translation between languages, and speech recognition” (Oxford Languages | The Home of Language Data, n.d.). Thus, the discipline of AI involves processes that collect knowledge and information while pretending or acting to be a human to use that learning to adapt to the different scenarios in the surroundings or new environments. Moreover, in its most naive form, AI is a discipline that syndicates the field of computer science and robust datasets comprising AI algorithms to enable problem-solving through “man-made computational devices and systems which would be inclined to call intelligent” (Brachman, 2005). In the contemporary world of technological advancement, there is still a lot of hope that surrounds AI development in product innovations for different arenas of life, with the peak of inflated expectations expected of any new emerging technology in the market or domain. Therefore, the expectations turn out in the bulk of advancement and development in the discipline of AI happening today by the industry leaders in the field of computer science (THORNBERRY, 2022). AI development utilizes human reasoning as the perfect replica of the human mind and intelligence to create better services for humankind.

Four Categories of Artificial Intelligence

AI precisely ascribes the feature of intelligence in different categories to find how to make machines solve kinds of problems, form concepts and abstractions, use or translate languages, and simulate machines on the intelligence that is reserved for human beings.

Decision Support Augmentation

In the field of AI, intelligence augmentation is actually the partnership between man and machine to lead, create, and innovate while contributing the strengths of both parties by leveraging machines to foster human intelligence. However, the idea of a partnership between humans and machines is not a new thing as J.C.R. Licklider proposed the “Man-Computer Symbiosis” partnership in 1950 in which humans are freed from their ability to be creative, and machines perform the revolutionized tasks while amplifying human abilities. However, the concept of augmentation is about “machines and humans being joined at the hip in a symbiotic relationship where each brings what it does best” (Freedberg Jr, 2015). It is to be believed that intelligence augmentation is the operating shadow of its sibling AI that offers a fruitful symbiotic relationship between human beings and machines. The partnership is to process and display human intelligence while contributing the strengths of each partner to take on the multiplicity of challenging tasks in the modern world of technology.

The use of enabling technologies such as intelligence augmentation through the use of AI provides insights into the generation, explanation, and improvement of data preparation is called predictive analytics and augmented analytics. The area of augmented analytics enabled by cloud technologies takes the best out of the world of emerging business intelligence in bringing decision-making to a level where important real-time data is produced for intelligent automated decision-making. Companies continuously generate new valuable data through the processing capabilities of people working in those companies to make balanced and rational business decisions with the minimum or zero possibility of human-made bias and errors. It is because, in the age of big data, critical business decisions are subjected to intelligent automated resources so making wrong decisions and biases can be costly. Thus, it is important that decisions should be based on unbiased and non-judgmental AI. This would increase the possibility that human beings can feel trusted, safe, and secure while sharing personal information with better possible outcomes to achieve a prime cognitive synthesis for the machines. A crucial part of this augmented intelligence or analytics system is its ability to collect complex data that is more personalized to each human through the pre-programmed specific principles to enhance insight during the decision-making process within the AI foundation (Freedberg Jr, 2015).

Digital Virtual Assistants Communicating through Natural Human Language

No individual in this world has enough capacity and cognitive skills to access, comprehend, or store all the information in existence because it takes a lifetime to fully comprehend and evaluate all perspectives of a single project only under high levels of cognitive complexity skills. There are heterogeneous perspectives about the immense size of the world, geographical positioning, cultural differences, socioeconomic history, and knowledge skills that can never be contested, let alone the unlimited mind space to comprehend a single human. To overcome this problem, AI has become our own virtual assistant for speech recognition that uses natural human language to communicate the answers to the queries requested by the users. It all starts with words when users “wake” words of their personal virtual assistants that are available on tablets, mobile phones, computers, and even on standalone devices, and they respond by listening to their users’ requests. The AI in those devices compares the request made by the user in the database, splits it into separate commands, understands the commands, and follows the actions provided by the database to find the correct output. These personal digital assistants exactly learn the way humans learn. For instance, if you have asked Siri to make a call to a person named George and she has dialed the number saved with the name Judge, you would tell it to “Stop,” and she would immediately understand that she has made a mistake. Next time, Siri will use this feedback for improvement, and better outcomes can be expected. This is AI as the assistant “Siri” used AI to understand human language, communicate with the in-built call function in your phone, wait for the response, and output the desired action. It means that these virtual assistants use speech recognition software and natural language processing to work effectively.

Natural Language Processing and Speech Recognition

It is the branch of AI that deals with building machines to recognize and react to words, texts, or voices in almost the same way a human being can. It interprets and manipulates human language in the form of voice data or text using software to comprehend the natural way of human communication. Speech recognition is a technology that allows digital voice assistants to convert input data in the form of voice to a format that is machine-readable. Several other translating software use the applications of AI integrated within other applications to translate a large amount of data into the language required by the user. In this regard, ML, natural language processing, and neural networking have played an important role in removing the language barrier. Speech recognition, also known as “Automatic Speech Recognition (ASR)” is an inter-disciplinary subfield of the computational linguistics that reliably converts voice data into text data (Reshamwala et al., 2013). In simple words, this system follows voice commands and responds in human language with the main benefit of searchability. This subfield of computer science and AI, specifically computational

linguistics, develops technologies and methodologies that categorize words, enable the recognition of voice and words, and convert speech into text. The virtual assistants decode the human voice, comprehend the message, and convert the voice into text with a certain confidence level to understand the human language in its natural form.

Voice to Text – Decision Automation Translation, Image Processing, and Classifying Content

Among the variety of domains in AI, voice-to-text is a significant feature within the speech service that accurately and quickly transcribes speech into text in different languages and variants in existence. Decision automation is an infrastructure that uses the rules and strategies of AI to help organizations or corporations automate decision-making through specific triggers. It is the use of software to convert speech into text to let organizations automatically make choices that could have been made by a human. Decision automation through the use of AI exposes decision-making technologies through which it codifies its principles for the NLP system. In terms of AI in decision automation translation, automation is an incredibly powerful tool that enables users to configure automatic projects based on the determined trigger to carry out follow-up actions. Furthermore, AI helps improve the user experience by classifying the requested content into a bucket category under the appropriate topics. Supervised automated text classification asks devices to imitate human intelligence by assigning a predefined label to perform data classification at scale. Classification of content into categories makes the whole process efficient and super-fast through the applications of AI with clear rules and algorithms of ML. Content classification is one of the most useful technologies that have enormous potential in the future because it is important to analyze and classify information through intelligent machine algorithms as more and more information is dumped on different websites over the internet.

Moreover, image processing is another engine room of AI automation that interprets the unstructured dataset captured through sensing, such as speech data, videos, and images. The technology that extracts the data from images for image processing through the application of a set of techniques and algorithms is known as optical character recognition and cognitive OCR. Image processing has further two sub-categories that include object detection and image classification. The former categorizes the pixels in the image to extract a kind of information from the image, and the latter identifies and locates the presence of an object in the image. [Facial and image recognition](#) in advanced devices are the hailed applications of AI that verify the face of an individual for unlocking the device. Image processing and AI in this regard can be seen as interdependent because AI models are mostly built upon image processing, and AI helps develop image processing through open-source libraries (Venegas-Andraca & Bose, 2003). In a nutshell, decision automation, voice-to-text transcription, image processing, and content classification go hand in hand because of the exponential increase in the availability of information found online.

Robotics and Advanced Products

The practical advances of AI and ML can be seen in robots, autonomous vehicles, and drones, which are the latest must-haves. In the next decade, drone driverless vehicles will be used to transport people and goods in a safe and efficient way. Autonomous vehicles use unreliable sensor data to make accurate predictions of the location of vehicles around the world. Such vehicles use a specific algorithm known as Simultaneous Localization and Mapping (SLAM) that employs a map to track the information regarding the quickest route while integrating all the algorithms between two points in the world. Similar to autonomous vehicles, robots use AI and advanced computer vision to predict and track the attitudes of human beings. These robots, after detecting humans' behaviors, plan their movements based on the observations, patterns of activities, and layouts of machines that help the system operate efficiently and safely alongside human workers in the warehouses. Each robot, through the applications of AI, is human-aware, self-optimized, and learns from self-collected, fully scalable data over time. Autonomous drones, also known as Unmanned Aerial Vehicles (UAVs), operate through two potentials, operational and navigation software to revolutionize flying machines (Freedberg Jr, 2015). The goal of autonomous drones through the use of AI is to unlock the full potential of flying machines for making efficient use of large datasets through data analytics and acquisition at the highest degree of automation. The utilization of complex ML and [deep learning approaches](#) is feasible for drones. Moreover, the neural network in drones helps computer vision to detect objects with a high level of accuracy, and in-built computerized programming such as GPS, sensors, cameras, navigation systems, and programmable controllers are the technological equipment an autonomous drone requires for automated flights.

Digital Ethics and Privacy by Design in Artificial Intelligence Systems

Privacy by design is a methodology embedded into the products that utilize AI throughout their developmental process. This methodology ensures that advanced products have embedded privacy principles that look for ways in which the personal information of individuals can be protected. Embedding privacy and ethics into technology poses several restrictions on how data is used, managed, transferred, and stored. AI and data ethics deal with payroll information about an individual or an organization that includes names, addresses, employees' codes, wages, and benefits that a person can anonymize to control who has access to personal data. In AI, privacy is at the core of what users and manufacturers do to secure the data. The power of the proliferation of virtual technologies presents certain ethical challenges that AI ensures to manage when it comes to handling, using, and sharing data. Digital privacy and ethics are all about fairness, integrity, and accountability in the embedded systems that focus on implementing high standards of data protection to see where there are gaps to be closed and biases to be mitigated (Felzmann et al., 2020).

Types of Learning in AI Systems

Learning models in AI systems can be classified into interactive types that AI utilizes in the design and development process for the real-world applications of AI systems today that are curated below:

Machine Learning

ML is a sub-field of AI that is more reliant on human involvement for learning from vast volumes of datasets. This application uses computer algorithms to train computers utilizing intelligence so that computers and digital devices can do things as per the capabilities that humans possess. To define, ML is the study of computer programs that leverage statistical models and algorithms without being explicitly programmed to evolve with each iteration (Allen, 2020). ML algorithms have the capability to update themselves through three prominent AI-based capabilities, which are as follows:

Artificial Narrow Intelligence

Artificial Narrow Intelligence (ANI) is the “weak” capability of AI that exists in this world of technology today. It is considered “weak” because it is programmed to perform only one task at a time in the real-time block, such as investigating the data to write a scholarly article. However, ANI capabilities can also pull information outside of the sole task they are assigned and designed to perform from the specific dataset.

Artificial General Intelligence

Artificial General Intelligence or AGI, are “strong” AI capabilities as compared to ANI that successfully perform any intellectual task that exhibits human intelligence.

Artificial Super Intelligence

Artificial Super Intelligence or ASI is a system based on the capabilities of AI that exhibit intelligence in almost every aspect from creativity and design to problem-solving and decision-making. This is the kind of AI that is expected to cause the extinction of the human race because of the potential of machines that are going to exhibit intelligence on their own.

Deep Learning

Deep learning is also a field of AI, but the sub-field of ML where “deep” refers to a neural network algorithm where deep learning eliminates several human interventions and automates feature

extraction piece of the process that enables the handling of larger datasets. Deep machine learning, also known as Scalable Machine Learning, leverages labeled datasets to ingest unstructured data in its raw form. This works on the principle of supervised learning to determine the hierarchy of features that do not require human interventions to process data. Moreover, supervised learning to inform the algorithm of deep learning allows the users to scale machine learning in more interactive ways (Allen, 2020).

Artificial Narrow Intelligence

Artificial Narrow Intelligence ANI in deep learning performs similar tasks as AI-based capability performs in ML. The subset of ML, deep learning, is goal-oriented in narrow AI as these “weak” AI-based capabilities are intelligent at performing and completing particular tasks. Narrow artificial intelligence uses natural language processing (NLP) such as voice and speech recognition, to understand human intelligence and execute tasks that are requested from narrow or weak AI systems.

Artificial General Intelligence

“Artificial General Intelligence” or AGI is also known as Deep AGI which is “strong” AI-based capabilities that emulate the human mind’s intelligence and mimic human behavior for solving varied problems in an effective and efficient manner. This network gives the device the ability to process information, learn human intelligence, and apply the learned approaches for contextual actions. Chatbots are examples of deep AGI that are basically the hypothetical intelligence of machines that are being taught to machines through multiple layers of near-simultaneous decision-making.

Artificial Super Intelligence

Artificial Super Intelligence, or ASI in deep learning, is capable of surpassing human intelligence. Many technological researchers believe that an advanced form of super AI systems can lead to a global catastrophe for humanity because of its technological advancement to surpass human minds and intelligence.

Neural Networks

Neural Networks, also known as “Artificial Neural Networks (ANNs),” have the ability to mimic the [human brain](#) and intelligence through a set of algorithms. It is the system of artificial nodes that are feed-forward in coherence with the actual brains of human beings. In simple words, these networks can flow in only one direction, from input to output, to mimic the intelligence of humans and other animals. The system can also backpropagate, which allows adjusting the algorithm in the opposite

direction from output to input while calculating and attributing the error associated with each node of the neuron (Allen, 2020).

Natural Language Processing

Natural language processing or NLP, enables devices to process human language through the use of other technologies such as deep learning models, ML, and computational and statistical linguistics. There are a few applications of NLP that include chatbots, prediction, speech recognition, and voice assistants, which are the main components of voice assistants. Chatbots are another application of NLP that have pre-programmed answering systems to respond appropriately to users' requests following specific patterns and rules while answering the questions that a user may have. Prediction, on the other hand, is the software that is one of the largest uses of natural language processing systems where a device suggests automatic prediction of the words that are being typed. The journey of understanding and recognizing the natural human language is where deep learning techniques come into the picture that focuses on improving new fronts for the interaction between machines and humans through text and speech (Reshamwala et al., 2013).

Knowledge-based Expert Systems

The knowledge-based expert system is an information system that normally would require human intelligence for problem-solving purposes. It comprises knowledge as data to help in problem-solving through drawing inferences from the knowledge base to involve the relationship between reasoning, knowledge representation, and learning models to build AI agents that would be capable of gaining insights into human-level intelligence.

Artificial Narrow Intelligence

Narrow AI is designed to perform specific singular tasks it is programmed to do. However, in expert systems, ANI involves a symbiotic relationship between man and machines for knowledge representations and learning methods to mimic the way humans think.

Artificial General Intelligence

Artificial General Intelligence or AGI in expert systems refers to the machines that realize true human-like intelligence when they are ready to be expected to solve problems, be imaginative, and make judgments while being artistic and ready to reason.

Artificial Super Intelligence

Artificial Super Intelligence (ASI) poses potential threats to the human race in the coming decades as AI-based capabilities develop thinking and cognitive skills of their own such as AI robots that may even enable artificial minds to be copied at a jaw-dropping pace.

Where is Artificial Intelligence Now?

Currently, AI-based systems are not capable of thinking at the human level but mimic animal intelligence to push the envelope of what AI and ML can do. However, AI's main challenges stem from bias due to bad privacy and ethics in different paradigms.

Machine Learning (Bias) vs. The Current State of Industrial Practice in Artificial Intelligence Ethics

As the field of ML is advancing, there are many biases and challenges highlighted in AI-based systems. In the current state of industrial practice, bias in ML stems from a tool that is used to assess parole of criminal cases through the software COMPAS which is currently used to assess the statistical information about how AI devices can form decisions. This software or tool successfully predicts recidivism in the datasets and algorithms for convicted criminals. These biases compromise AI ethics in industrial practice and are the result of the datasets but are classified as the source of data used for the creation of an AI model at hand. Data is commonly cleansed before testing an ML model in industrial practice, but humans unconsciously amplify bias in the model, which is called prejudicial bias and exclusion bias. During production at the industrial scale, measurement bias occurs when the data is collected for training with different paradigms and characteristics. Lastly, algorithmic bias stems from the ML model itself, which results in unfair machine outcomes (Choudhury et al., 2020).

Digital Ethics Comprises the Systems of Values and Moral Principles for the Conduct of Electronic Interactions among People, Businesses, and Things

Personal digital ethics of AI drive the values and moral principles for the conduct of electronic interactions and the growth of organizations. These ethics encompass how people and businesses honor each other's right to self-determination in the online world. Digital principles and ethics in AI-assisted systems describe interactions, behaviors, intentions, and decisions that shape the practices and electronic interactions of every individual, entrepreneur, and business within the realm of technology. The ethical practices build the transformative impact on the delivery of effective AI-based

models and services to people and organizations. Contrary to this conduct, if these ethics become blurred between the digital and the real world, the real world of human beings would greatly be affected due to ethical breaches in digital transformation.

Comprehensive Socio-Technical Approaches to (TEVV)

Socio-technical approaches have an important part in enhancing the performance of AI-assisted models through testing, evaluation, verification, and validation approaches. To achieve complex TEVV bias in the systems assisted by ML and AI, mass customization of AI models is used to ensure the effective interaction between machines and humans. Socio-technical approaches mitigate the bias in the AI models and establish a new culture change that enhances the performance and ensures the adaptability of new technologies in any industry.

Decision Automation

Augmenting the decision automation support through human intellect, industry leaders refer to a way of life in an integrated mean where a man's capability to derive effective and relevant solutions for problems is enhanced through high-powered electronic aids and sophisticated, streamlined methods. Therefore, the idea of augmenting a new path to the decision is not about machines working autonomously alongside humans but the concept of machines replacing humans in almost every field of life.

Bias-Detection

In ML, bias can be detected at the first stage of data collection because of the reason datasets are usually created and collected through human inputs. The bias found in this stage is selection bias which has the "framing effect" as diversity is introduced and represented in the datasets at this developmental yet influential stage. Another bias that can be detected in the first stage of data collection is a systemic bias which is extremely difficult to detect in AI-based systems because it is a repeatable and consistent error in ML. If this error is not detected in the initial stage, faulty machinery will be the end result of the AI operational process. To alleviate bias in machine-based models, "Local Interpretable Model-Agnostic Explanations (Lime)" are used to comprehend why the model at hand detects a certain bias by computing the relative importance of the inputs of AI-based models (Choudhury et al., 2020).

Bias Mitigation Tools

The systemic bias, which is a difficult bias to detect in the AI data collection stage, if found, can easily be mitigated by maintaining a good understanding of the hardware and coding that are used in the production of the AI system at hand. Moreover, responsible licensing practices can be adopted to prevent high-risk AI-based models from being leveraged to prohibit the harmful use of AI for [mass surveillance](#). Open-sourced AI software can be adopted to limit the use of potentially irresponsible and harmful AI systems through voluntary licensing framework tools by the individual developer of the model.

Applying Software Assurance (SwA) to AI

Oftentimes, initiatives of AI fail due to unfamiliar paradigms, security breaches, trust issues, lack of best practices in terms of software engineering, and high time pressure. To mitigate these problems, software assurance can help develop and apply a unique set of policies to keep software configurations safe, protected, and up to date. Software Assurance, in this regard, is the justified confidence that is inserted as part of the AI system in a product that is free of exploitable vulnerabilities. In the discipline of AI, alongside the field of computer science, the code quality and solid engineering to design, build, and deploy AI systems are difficult but are essential for the success of responsible AI. Software assurance transforms an engineering effort into a practical application by conducting in-depth assessments of AI processes and software that provide insight into the maturity of software and solutions that support robust legal and ethical compliance. The assurance (SwA) also offers improvement guidance to manage testability and changeability for the continuous transparency of AI systems development (Freeman et al., 2022).

AI Improvements using Software Assurance (SwA)

Software Assurance (SwA) strengthens the processes and methods to empower the software industry with the latest technologies to deliver a faster time to the emerging market of technology and a better customer experience. SwA expedites the testing processes of the software to perform high-level quality checks on the products based on AI systems (Freeman et al., 2022). It is the most promising technology that will help the embedded AI-based systems to overcome varied challenges of privacy, implementation strategies, and adaptable algorithms in AI specifically in ML. Software Quality Assurance detects errors and bugs instantly in real-time AI systems and makes it easy for any software to leverage AI in its processes.

Algorithms and Related Tools Usage (Development Artifacts)

Software Assurance (SwA) organizes and incorporates multiple artifacts with the purpose of making, establishing, and developing software systems in AI products to foster the processes of development in a manageable, secure, and intelligent manner. The engineering set of SwA utilizes different tools to form an idea regarding the evolving quality of the artifact sets that include tools for design, implementation, development, and management sets. Firstly, to engineer design models, visual tools with different levels of abstraction are used which mostly include software architecture descriptions, design models, and test models. Tools that are used for design sets include Unified Modeling Language (UML) notations that visualize the way a system is designed. Secondly, test management tools for software assurance are used, which include code analyzers, debuggers, and compilers that contain executable source code for standalone testing of AI components such as form and interface. Thirdly, network management tools are used for the development of SwA that including tools for test automation and coverage. These tool sets for the development artifacts contain installation scripts and ML notations to use the AI product in its environment where it is supposed to be used. Lastly, the management set uses various artifacts such as software development plan, work breakdown structure, deployment of the business case, and environment where the AI product is expected to be used.

Increased Rigor to Support the Secure Use of Technology

AI is driving improved efficiency due to the evolving chatbots and ML in the field of technology. Several technological implementations such as chatbots, biometrics, deep learning platforms, cyber defense, robotic process automation, image recognition, and decision management support the secure use of technology and rocking the world through logic and effective decision (U.S.G.A, 2022). Chatbots interact with humans and biometrics, making sure that technology can identify and analyze attributes and features of the human body. Robotic process automation furthers the security game as it mimics the human process using scripts that are fed to a machine to complete its automation task effectively. Moreover, cyber defense acts as a firewall that provides timely support to prevent any threat and, if found, fight against it so that it cannot affect the infrastructure of the AI-based systems. Image recognition is another security measurement that recognizes and distinguishes a trait in a virtual image that increases engagement and improves security and performance.

Automated Security Best Practices for AI

The level of cognitive automation security practices in AI-based products is so high that developers and manufacturers of those systems need not be afraid of security or privacy system leaks. Automated security is the core component of digital transformation initiatives throughout the world to improve compliance, quality, accuracy, and productivity of data sets that are used to empower machines that imitate human intelligence. Best practices for AI automated security are defined as operational processes that are secure and most effective. Traditional software attack vectors are critical to addressing, but security problems need to be mitigated to fight an uphill battle against AI adversaries (Brundage et al., 2018). Firstly, operations foundation and secure development must incorporate discretion, authentication, and resilience when protecting AI and the datasets under AI control. AI must have built-in forensic capabilities in all systems to recognize bias in AI's interaction with humans that would help identify and resolve root causes of the bias in ML and deep learning. Moreover, AI must be capable of discerning and recognizing maliciously introduced datasets to safeguard sensitive information and resolve complex problems in ML (Barreno et al., 2010).

Current Research Efforts

The use and implementation of AI in a variety of research fields have been speeding up over the past few decades with the advancement of AI technology and multiple digital revolutions. NIST develops different tools and fundamental standards to foster research efforts in different areas, including engineering biology, robotics, medical imaging, natural language processing, [disaster resilience](#), computer vision, quantum physics, and advanced communication technologies. Current research efforts in different fields of life that address the complex intertwinement of trustworthy AI and its different aspects are as follows:

Academia

Over the past few decades, AI and ML have drastically improved the field of academia and have enhanced the professional growth of individuals who seek societal and academic challenges with the support and use of AI technologies. The adaptive technologies of AI and ML to support data-driven scientific hypotheses enhance the access to datasets available online at an unprecedented speed. The increasing demand for the concepts of AI and ML has led to a hard-fought competition between different academic paradigms across the world that has substantially transformed the academic industry. AI-enabled processes concerning natural language processing patterns allow researchers to quantify computational linguistics to mitigate negative terms in language for identifying flawed results and statistics. Moreover, AI-enabled technologies through scientific collaboration pave the way for open-source science that allow academia to join forces through inclusive approaches of global scientific platforms.

Industry

Market research applying AI techniques such as wireless network control systems, advanced material discovery, and robotic systems in environment manufacturing are the major demands in the industry. Worldwide industries are using market research with AI sub-disciplines for the collection and collaboration of data as well as automation of tasks through ML and natural language processing technology. In global industries, AI-enabled technologies are used to process surveys so that industries or corporations can find customized questions, collect the data, analyze the information provided, and provide the answers. Currently, it is also used in marketing strategies to make, implement, and process business decisions faster through collaborating the researched data according to the market needs with the sales and behaviors insights.

Government

The ever-emerging field of AI has successfully paved its way from the research lab to the world of business to the local and global governments in just a span of the past few years. The investment of AI-powered technologies in local governments such as data insights, chatbots, and smart cities has been transforming government bodies and related agencies for the better. The use of AI in governments has improved privacy, legacy systems, security concerns, and evolving workloads that have solved the most complex problems in modern society. Advanced research and development in governmental sectors can support critical capabilities through the combination of analytics power, AI, and high-performance computing (HPC) to help improve situational awareness and decision-making among global government bodies. For example, government-funded research in the field of medicine can help AI algorithms enable cheaper and faster predictions of the sequence of amino acids in terms of 3D protein structures that can help in the diagnosis of diseases as well as the designing of drugs to treat chronic illnesses.

Gaps that Exist in Artificial Intelligence

As the field of AI is emerging with time, it raises the concern of how AI-enabled systems will impact societal values, cultural differences, and public privacy and security. The highly autonomous behavior of AI-enabled systems such as robots and autonomous vehicles, for which neither the operator nor the programmer seems to be responsible for the potential threats such autonomous systems can cause, has been suspected to enhance gaps in responsibility and accountability. These responsibility and accountability gaps can incentivize harmful behavior due to the system's self-sufficiency to function autonomously from the human interference in decision-making and management processes. These gaps occur in AI-based systems due to the fact machines do not get concrete human instructions. At the same time, machines also do not deem agent-like or sophisticated responsibility bearers of the damage caused to the environment, society, or people. This cancels people's responsibility and

precisely is a “gap” in responsibility not because of the absence of someone but because of the discrepancy and lack of accountability. Moreover, the capability gap supports warfighters that prevent the AI from achieving the desired goals that need to rectify the strategy and performance. The capability gap blends warfighter expertise with quantifiable statistical methods through a scientific approach. These gaps compare the objective requirements and threshold assessing the potential solutions with the warfighter-identified optimal and good-enough values.

Future of Artificial Intelligence

AI operating along with the advancements in the field of computer science has shaped the future of humanity across nearly every field and industry around the globe. The pace of evolution in this era due to AI-enabled technologies and systems is faster than ever because of robotics and big data mimicking human intelligence in all cognitive tasks. The advancements and innovations due to AI are diversified in almost all industries from healthcare to education, military, finance, and cybersecurity. The systems assisting through AI, ML, and deep learning can improve the quality of life to a great extent acting as a technological innovator for the foreseeable future. However, AI-assisted systems can be a curse for humanity if it reaches the wrong hands that can use technological advancements for accomplishing their own nefarious designs. The development of the world depends on the quality of technological advancements that can boost the economic, financial, and security of global systems. The future of AI is going to transform the world through automation and robots surpassing an individual's ability and personality where even industries do not need skilled laborers. AI has taken the central stage since the emergence of model-and-algorithm-based ML that has the ability to harness learned intelligence and massive amounts of data for making optimal discoveries in the field of technology. Thus, AI would not cede the spotlight in any fraction of the time soon like never before.

Recommendations

It is not easy in today's era of new advancements in different paradigms to predict the future of AI for the next decades. Programmers and manufacturers of AI-assisted systems are concerned to construct human-like machines and they are successful somehow as computer science through the applications of AI has boomed in robotics. Neural networks in this regard are the hottest area of ML and AI that work on natural language processing and voice recognition. Researchers and programmers can center their studies and work in the field of neural networks along with advancements in ML to perpetuate bias in AI so that machines can perform what humans do. This study recommends contributing more to the field of neural networks and AI as no computer is showing full AI to date

References

Allen, G. (2020). Understanding AI technology. Joint Artificial Intelligence Center (JAIC) The Pentagon United States.

- Barreno, M., Nelson, B., Joseph, A. D., & Tygar, J. D. (2010). The security of machine learning. *Machine Learning*, 81(2), 121-148.
- Brachman, R. J. (2005). Getting back to" the very idea". *AI Magazine*, 26(4), 48-48.
- Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitsoff, T., & Filar, B. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *ArXiv Preprint ArXiv:1802.07228*.
- Choudhury, P., Starr, E., & Agarwal, R. (2020). Machine learning and human capital complementarities: Experimental evidence on bias mitigation. *Strategic Management Journal*, 41(8), 1381-1411.
- Felzmann, H., Fosch-Villaronga, E., Lutz, C., & Tamò-Larrieux, A. (2020). Towards Transparency by Design for Artificial Intelligence. *Science and Engineering Ethics*, 26(6), 3333-3361. <https://doi.org/10.1007/s11948-020-00276-4>
- Freedberg Jr, S. J. (2015). Centaur Army: Bob Work, Robotics, and the Third Offset Strategy. *Breaking Defense*, 9.
- Freeman, L., Batarseh, F. A., Kuhn, D. R., Raunak, M. S., & Kacker, R. N. (2022). The Path to a Consensus on Artificial Intelligence Assurance. *Computer*, 55(3), 82-86.
- McCarthy, J. (2004). What is artificial intelligence. URL: [Http://Www-Formal. Stanford. Edu/Jmc/Whatisai. Html](http://Www-Formal.Stanford.Edu/Jmc/Whatisai.Html).
- McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955. *AI Magazine*, 27(4), Article 4. <https://doi.org/10.1609/aimag.v27i4.1904>
- Newell, A., & Simon, H. A. (2007). Computer science as empirical inquiry: Symbols and search. In *ACM Turing award lectures* (p. 1975).
- Oxford Languages | The Home of Language Data. (n.d.). Retrieved December 23, 2022, from <https://languages.oup.com/>
- Reshamwala, A., Mishra, D., & Pawar, P. (2013). REVIEW ON NATURAL LANGUAGE PROCESSING. *IRACST - Engineering Science and Technology: An International Journal (ESTIJ)*, 3, 113-116.
- Venegas-Andraca, S., & Bose, S. (2003). Quantum Computation and Image Processing: New Trends in Artificial Intelligence.
- U.S.G.A. *Artificial Intelligence: DOD Should Improve Strategies, Inventory Process, and Collaboration Guidance*. Retrieved December 28, 2022, from <https://www.gao.gov/products/gao-22-105834>

THORNBERRY, W. M. M. (2021). NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2021. *PUBLIC LAW*, 116, 283.