AI’s Modern Development

Christopher Faustino

IT 104

9/27/23

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on https://catalog.gmu.edu/policies/honor-code-system/ and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of 2 text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on https://universitypolicy.gmu.edu/policies/responsible-use-of-computing/ web site."

AI’s Modern Development

Introduction

Artificial Intelligence (AI) is a groundbreaking technology with vast transformative potential, particularly in the field of security. AI's unparalleled ability to process extensive datasets and recognize patterns at incredible speeds enhances threat detection and decision-making to an unforeseen level. While it has already proven invaluable in cybersecurity, its integration into our daily lives raises very concerning questions that encompass security, ethics, and society. Security is a paramount concern as AI's vulnerabilities may be exploited for malicious purposes. Ethical questions surrounding AI's capacity to automate jobs and influence decision-making highlight the need for fairness, accountability, and transparency. The widespread adoption of AI also has the possibility to reshape society, impacting employment and redefining notions of privacy and autonomy in unprecedented ways. Therefore, it is important to examine AI's multifaceted growth, emphasizing responsible and ethical development and implementation.

AI’s Current Use

In recent times, the utilization of Artificial Intelligence has surged significantly, reaching various domains. Its transformative potential spans across diverse sectors, including education and urban planning. In education, AI offers personalized learning experiences by providing instant feedback and adapting instructional content to individual student needs. This not only benefits students but also supports teachers in engaging learners more accurately and effectively. AI can also be used to augment and better conceptualize more complicated ideas for both students and faculty, as stated in the following quote: “Throughout every stage of their work, engineers generate and utilize a vast quantity of documents. Hence, engineering students and faculty can use large-scale language models like ChatGPT and Bing Chat to improve their productivity, creativity, and quality.” (Goel 2023). In urban planning, AI aids in informed decision-making by analyzing extensive data on traffic flow, energy consumption, and public transport. It optimizes city services and infrastructure, enhancing urban life. AI also extends to predictive modeling and automation, optimizing city services like waste management and traffic control for increased efficiency and sustainability. For instance, AI-driven waste management optimizes collection routes, reducing emissions, while smart traffic control improves air quality and reduces congestion. AI has also been used to aid in blight detection in urban areas, urban blight standing for cities or towns that are in a state of disrepair or decay. Garbage trucks are used to survey and capture images of urban areas, the trucks park in a lot and upload the data through Wi-Fi, AI then uses those images to generate a blight score which represents that city's degree of decline. This process, if implemented, could aid in the maintenance and upkeep of various cities and towns across the country, preventing them from falling into severe disrepair. However, the AI must first be trained with images from various sources, which has its own set of problems, “The substantial amount of training data that AI models require can pose a challenge to organizations that do not have a robust photo inventory.” (AI IN CURRENT PRACTICE 2023).

Security Points

The advent of Artificial Intelligence has unquestionably ushered in a brand new era brimming with possibilities across various domains. However, as with any transformative technology, it ushers in a wave of very complex challenges that demand our time and attention. In the intricate landscape of cybersecurity, AI has emerged as a very formidable ally, lending its abilities to the development of cutting-edge security strategies. One of AI's key strengths lies in its ability to analyze vast datasets and swiftly identify intricate statistical patterns that human analysts might overlook. This analytical prowess enables AI systems to detect anomalies, pinpoint vulnerabilities, and predict potential threats with incredible accuracy. Thus, it plays a pivotal role in boosting our digital defenses against the ever-evolving tactics employed by cybercriminals, “”We see AI as an integral part of cyber security strategy.’”” (Srikanth 2023). Nonetheless, as AI becomes more deeply intertwined with decision-making processes in the cybersecurity domain, a potential vulnerability emerges. Malicious individuals, often ingenious scammers, could exploit this vulnerability by manipulating the data ingested by AI models. These subtle alterations might lead AI systems to make erroneous decisions, inadvertently aiding cyberattacks rather than thwarting them. This emerging back and forth between cybersecurity experts and malicious agents underscores the critical importance of securing the integrity of AI systems themselves. Beyond data manipulation, scammers have ingeniously harnessed the power of AI to craft malware that continually mutates and evolves. These AI-driven malware strains are adept at shape-shifting to evade conventional detection mechanisms. Consequently, because of the accessibility of AI, it poses a significant challenge for cybersecurity experts tasked with identifying and neutralizing these threats as it opens the door to more user generated malware in the open, “"Now, it mostly allows people who are not software developers to create malware. That makes the threat higher because at the end of the day there will be more malware criminals in the wild and more malware criminals will try and attack corporations."” (Dinzeo 2023). The dynamic nature of AI-driven threats necessitates continuous adaptation and innovation within the cybersecurity community. Countermeasures must not only keep pace with the evolving tactics of cybercriminals but also anticipate their next moves. To address this challenge, cybersecurity experts are increasingly turning to AI's own capabilities, utilizing machine learning and neural networks to develop more sophisticated and adaptive security systems.

Ethical and Social Implications

The rapid development and integration of Artificial Intelligence has indeed ushered in a new era, but it has not been without its ethical and social dilemmas. One of the most pressing concerns revolves around AI's capability to automate and potentially replace jobs that have traditionally been performed by humans. This phenomenon has generated substantial apprehension regarding the possibility of widespread unemployment in various fields and industries. While it's reassuring to see that many employers are currently placing a strong emphasis on job security, with companies such as Securonix being one example, the relentless advancement of Artificial Technology inevitably poses a challenge to the status quo. As AI continues to evolve and prove its effectiveness in completing tasks, employers may find themselves increasingly compelled to explore the benefits of automation. AI can perform tasks with unmatched precision and consistency, making it an attractive option for businesses wanting a more cost effective way to streamline their operations. As a result, there's a growing inclination among employers to integrate AI into their workflows, raising questions about the future landscape of human employment. Consequently, businesses, and society as a whole must engage in proactive discussions and measures to mitigate the potential consequences and ensure that the benefits of AI are harnessed responsibly and inclusively. This entails not only addressing the challenges of potential job displacement but also consider how AI can complement human capabilities. Solutions must encompass addressing job displacement while fostering collaboration between humans and AI, with AI handling repetitive tasks and humans focusing on creativity and critical thinking. This quote is an excellent overview on AI in the workforce: “”There needs to be a human being to really validate whether that is real or not. We cannot just exploit AI to automate everything because we will have a huge job crisis in the country. So there are regulatory aspects, there are regional, cultural aspects.”” (Srikanth 2023). Lifelong learning and adaptability are essential attributes for the future workforce. In addition to employment concerns, AI's societal implications extend to issues such as bias and fairness in AI algorithms, data privacy, and the ethical use of AI in decision-making processes. As AI systems continue to learn from vast datasets, there is a risk of perpetuating biases present in the data, which can result in discriminatory outcomes. Ensuring transparency and fairness in AI algorithms and practices is crucial to building trust and addressing these ethical concerns.

AI’s Future Use

As AI technology continues to advance, we can anticipate seeing Artificial Intelligence become increasingly integrated into various parts of our daily lives. This trend is already evident with more smartphone companies, such as Apple and Samsung, incorporating facial recognition capabilities, enhancing the security and convenience of our personal devices. Beyond biometric authentication, AI's potential extends into the realm of customer service and support, where intelligent chatbots and virtual assistants are expected to revolutionize how we interact with businesses and receive assistance. In the not-so-distant future, AI-driven systems like ChatGPT are expected to play a pivotal role in delivering personalized and efficient customer experiences. These models, with their natural language processing capabilities, can understand and respond to questions made by humans with remarkable precision, reducing response times and ensuring consistent service quality. This evolution in customer service is just one example of how AI is expected to simplify and enhance our daily lives. As we look ahead, it's clear that AI's future is a bright one, filled with promise and innovation. Models such as ChatGPT are at the forefront of this technological revolution, and their ongoing development will continue to shape the landscape of Artificial Intelligence. With each advancement, we draw closer to a world where AI seamlessly enhances our lives in ways we might have never imagined. Therefore, it's safe to say that we won't be hearing the last of Artificial Intelligence anytime soon, as it continues to reshape and enhance our daily experiences.

Reference Page

CHAPTER 3: AI IN CURRENT PRACTICE. (2023). Planning Advisory Service Report, (604), 26-41. Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/trade-journals/chapter-3-ai-current-practice/docview/2829265971/se-2

The article highlights the significant role of Artificial Intelligence in urban planning and management. It identifies four key AI application areas: machine learning, computer vision, natural language processing, and artificial neural networks. These areas enable computers to learn, perceive, understand human language, and make decisions based on data. The integration of these AI tools empowers planners to analyze large datasets, identify patterns, and make informed decisions for urban development. Additionally, the article emphasizes the potential of AI-driven smart city technologies to automate and enhance various services, promoting self-sustainable urban environments.

Computer, E. (2023). Scamming the scammers: New AI fake victims to disrupt criminal business model. Express Computer, Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/trade-journals/scamming-scammers-new-ai-fake-victims-disrupt/docview/2829918479/se-2

The article discusses the development of Apate, an AI-driven system designed to combat phone scammers. Apate employs multi-lingual chatbots with convincing voice clones to engage scammers and waste their time. Phone scams are on the rise due to easy masking of call origins and the difficulty of improving call authentication. Apate's chatbots are trained on real scam conversations using machine learning and natural language processing, effectively posing as

scam victims and reducing successful scams. The chatbots also contribute to threat intelligence, and the technology has the potential to disrupt the scam industry through partnerships with telecommunications providers.

Goel, S. (2023). How AI and ChatGPT can embrace engineering education? Express Computer, Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/trade-journals/how-ai-chatgpt-can-embrace-engineering-education/docview/2789772529/se-2

The Article discusses the transformative role of AI in education, particularly in engineering education. It highlights the use of large language models like ChatGPT and Bing Chat to enhance learning experiences for students and support faculty members. These AI platforms assist in various tasks, from providing feedback to improving writing skills. The source recognizes the challenges of AI in education, including issues related to bias, discrimination, privacy, security, ethics, and costs. It emphasizes the need for maintaining intellectual challenges in learning while leveraging AI tools to drive quality, innovation, and productivity in engineering work.

Srikanth, R. P. (2023). We see AI as an integral part of cyber security strategies: Ajay biyani, securonix. Express Computer, Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/trade-journals/we-see-ai-as-integral-part-cyber-security/docview/2796409554/se-2

Ajay Biyani, Vice President at Securonix, discusses the company's innovative approach to threat detection and automation in enterprise security. Securonix differentiates itself by building both UEBA and SIEM platforms from scratch, ensuring seamless integration and minimal disruptions during upgrades. They offer comprehensive solutions, allowing analysts to visualize threat chains and correlate compromised firewalls with machine identities. The company is pioneering cloud-based data lakes and next-gen solutions, including autonomous threat detection. While AI plays a crucial role in cybersecurity, human intervention remains vital, and ethical considerations and regulations are significant in its use.

Dinzeo, M. (2023). Cyberattacks are accelerating with AI's help. BenefitsPRO, Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/trade-journals/cyberattacks-are-accelerating-with-ais-help/docview/2824117950/se-2

This article highlights the growing threat of cybercriminals leveraging large language models, such as ChatGPT, to supercharge their attacks. Experts warn that AI tools, once used for security, are now being employed maliciously. It cites a case where a malware writer used OpenAI's GPT to create a new virus, showing the evolving sophistication of AI-driven cyberattacks. Additionally, AI streamlines phishing attacks by generating convincing emails impersonating trusted institutions. Organizations are advised to incorporate AI into their security strategies and educate employees to identify potential threats in this ongoing cybersecurity arms race.

Criddle, C., & Staton, B. (2022). AI breakthrough ChatGPT raises alarm over student cheating. FT.Com, Retrieved from http://mutex.gmu.edu/login?url=https://www.proquest.com/trade-journals/ai-breakthrough-chatgpt-raises-alarm-over-student/docview/2765934592/se-2

This article discusses the rising concern in the academic field about students using AI, such as ChatGPT, to create essays. Academic experts worldwide are advocating for new methods of assessment to combat academic dishonesty facilitated by AI. ChatGPT, created by OpenAI, can generate convincing text, but it often requires fact-checking. It also mentions concerns about the free accessibility of such AI tools and their impact on the need for resources to evaluate content. The source reports on a seminar by JISC that emphasized using AI to enhance creativity rather than engage in a "war" with plagiarism detection tools.