One of the most transformative applications of computing in recent years is the integration of AI-powered assistants in business operations. Companies like OpenAI, Google, and Microsoft have developed AI tools such as ChatGPT, Google Bard, and Microsoft Copilot, revolutionizing customer service, workflow automation, and content generation.

For example, PwC (PricewaterhouseCoopers) adopted AI assistants in 2023 to enhance their internal knowledge management system, allowing employees to retrieve real-time insights, automate reports, and improve productivity. Similarly, Amazon uses AI-driven algorithms to predict customer preferences and optimize logistics, significantly improving efficiency and customer satisfaction.

This case study highlights how computing disciplines, such as AI, software engineering, and data science, converge to create intelligent, automated solutions that drive business success. It also underscores the ethical concerns of AI implementation, including data privacy, job displacement, and biases in AI models.

Discussion Points

How does AI-powered automation transform businesses?

Answer:

Many fields across a wide range of industries have been transformed by the rise of AI and the emergence of AI-powered automation.

That has contributed to simplifying processes, reducing costs, increasing efficiency and much more.

Such contributions could be seen in areas of research and development where for instance complex research tasks were simplified using AI-powered simulation technologies reducing dependency on resources and methods that had previously required much time and cost to perform.

Furthermore, there has been a shift towards the use of AI-powered automation in customer support, administrative and operational tasks. This encompasses RPA (Robotic Process Automation), chatbots and AI agents, which can perform a wide range of tasks, from straightforward and simple ones, up to more complex ones.

The use of AI agents in cyber security is leading to the development of automated, proactive and adaptive threat detection and response capabilities. This represents an advancement from more limited methods, such as signature-based detection and response. The most significant benefit of this approach is the reduction of reliance on human nature-based detection and response, which may be more prone to error due to human nature.

However, AI-powered automation is also not perfect and has its own drawbacks and most probably would produce similar negative effect if not trained and implemented correctly and efficiently.

(Gonçalves, and Domingues, 2025)

In addition, implementing cost-effective, efficient and effective solutions demands expertise in many fields, including IT, privacy laws and legislation and much more.

What ethical concerns arise with AI adoption in business operations?

Answer:

Technological progress is already introducing a future where advancements in artificial intelligence, data collection and analysis will continue to grow. Similarly, there will be an increasing collection of data for the purpose of individualized marketing, this could have an additional negative effect on privacy protection. With the digitalization of much of today's life, it is reasonable to assume that this trend is on the rise and will most probably continue to arise. There is already some suggestions that AI may be in violation of privacy, copyright and intellectual property laws.

This raises significant concerns about such and other aspects of privacy implications, which are of great concern.

(Lucchi, 2024)

At the same time, there is the continued need to rely on technology to secure democratic and constitutional processes, while at the same time this underscores the fundamental importance of protection of individual privacy and liberty. Achieving this requires careful attention to the relationship between these two aspects — a challenge that requires a balanced technical, philosophical, legal and ethical approach.

It is possible to mitigate some risks, but not all, by using various techniques. These include the use of random data such as, for instance, the proper handling of elements like quasi-identifiers and direct identifiers, mathematical options such as differential privacy, and the like. Nevertheless, the course of technological advancement in recent years has shown on several occasions that there is no complete guarantee that full privacy protection can be ensured while allowing the intended use and accuracy of the data.

(Raja, 2024)

Privacy protection will most probably continue to become an increasingly challenging aspect of the life of most people in today's digital age.

How do different computing disciplines (AI, cybersecurity, software engineering) contribute to AI-powered assistants?

Answer:

Artificial intelligence is becoming more present in cyber security. for instance, Vendors such as Splunk (which now owned by Cisco), have incorporated AI into their Security Operations Centre (SOC) and security orchestration, automation and response (SOAR) products very early. Another example is GitHub, which integrated AI-Automation futures called Copilot into their software engineering line of products.

This has contributed to automating processes like threat detection and response, software development, education enhancement, vulnerabilities detection and remediation, both on computer code level and across the infrastructure. Vendors from a variety of fields are increasingly adopting this approach.

This advancement has been criticized on the grounds that it may result in some people learning less efficiently by over-relying on AI automation rather than learning the fundamentals of specific technical roles. for instance, in the area of computer engineering, there may be a tendency to priorities vibe coding over learning to code.

The use of AI-powered automation in the Security Operation Center (SOC) is another example of such an area where experts may over-relay technology instead of developing skills. Such reliance could lead to deficiencies in cyber events detection, for instance as an excessive number of false positives, or even more serious, true negatives not being effectively identified and addressed due to over reliance on AI-Automation. It is important to note that there is no single approach that is alone effective. What works best is a combination of different methods that are adapted, specifically tailored and fine-tuned to suit the situation.

References.

Gonçalves, R. and Domingues, L., (2025). Artificial Intelligence Driving Intelligent Logistics: Benefits, Challenges, and Drawbacks. *Procedia Computer Science*, *256*, pp.665-672.

Lucchi, N., (2024). ChatGPT: a case study on copyright challenges for generative artificial intelligence systems. European Journal of Risk Regulation, 15(3), pp.602-624.

Raja, V., (2024). Exploring challenges and solutions in cloud computing: A review of data security and privacy concerns. Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, 4(1), pp.121-144.