Navigating Automation in IT: My Professional Reflections, Industry Impact, and Future Trends

Good day, I am delighted to welcome you to this presentation on "Navigating Automation in Enterprise IT: Professional Reflections, Industry Impact, and Future Trends."

Brief Overview of the Presentation: This presentation aims to offer insight into my reflections and professional encounters with automation in Enterprise IT and to explore its impact on my career.

The core technologies of automation integrate into existing systems, thus impacting various industries and transforming job roles and skill requirements. However, ethical considerations regarding widespread adoption also arise.

Automation is pervasive in virtually every facet of enterprise IT. It encompasses tasks from basic tasks like ticket generation in IT support to more complex functions like analysing patterns and indicators to predict and determine cybersecurity breaches. Within enterprise IT, technology is leveraged to execute operations with minimal human intervention, thus amplifying efficiency and reshaping occupational functions across diverse sectors.

IT Service Desk

“When a ticket is produced, its categorisation and routing to resolving experts are tasks of the utmost importance” (Zangari et al., 2023).

Commencing at the stage where most individuals enter the IT sector in the workplace is the helpdesk. Automating the case-based help desk support system offers numerous advantages, such as heightened efficiency, consistency, and accuracy, and facilitating knowledge sharing and collaboration. Moreover, it fosters improved decision-making and

knowledge preservation. Additionally, it yields time and cost savings, scalability, and continuous improvement.

“The AI chatbot service has reduced waiting lines at call centres, allowing human attendants to solve complex issues, contributing to a more efficient service” (Martins et al., 2021).

Use of Chatbots in IT support

“Chatbots are the new apps” (Kühnel et al., 2020). This declaration, made eight years ago by Satya Nadella, CEO of Microsoft, anticipated the critical role of human oversight in IT automation. Since then, the technology landscape has evolved significantly, with a notable rise in the use of chatbots. These AI-driven tools have revolutionised customer service and IT support by providing instant, automated responses to user queries, enhancing efficiency and user experience.

However, this surge in automation also underscores the ongoing relevance of human intervention. While adept at handling routine inquiries, Chatbots often require escalation to human agents for more complex issues, reflecting the persistent need for human judgment and adaptability. "Rule-based approaches, unlike data-driven ones with extensive labelled training data, are prone to individual biases and may lack robustness due to inconsistencies from different designers"(Samarakoon et al., 2011).

This trend illustrates the broader theme in IT service: as automation capabilities advance, the balance between automated systems and human oversight remains crucial, ensuring that while efficiency and speed are maximised, the nuanced understanding and ethical considerations human operators provide are not compromised. Chatbots significantly contribute to automation, increasing efficiency and lowering costs. “By leveraging these

technological advancements, organisations can streamline their operations, improve customer satisfaction, and achieve cost savings in the long run" (Aslam, 2023).

There are, however, several concerns regarding the use of chatbots, more so in mission-critical situations.

Integrating automation into help desk ticketing processes has presented challenges, particularly regarding reliability. There is also "a concern with regards to security" (Rapp et al., 2021).

Reflection on Automation in IT Support

In my professional experience, integrating IT Service Management (ITSM) systems with artificial intelligence (AI) has significantly addressed various operational challenges. This integration leverages AI's capability to process and analyse vast amounts of data, enhancing the quality of input data. Consequently, ITSM systems can produce more accurate and reliable outcomes, which are crucial for maintaining high service standards and ensuring efficient problem resolution.

A notable improvement from this integration is in helpdesk operations. AI-driven ITSM systems streamline ticket creation by automatically categorising and prioritising issues based on their content and urgency. This automation reduces the workload for helpdesk staff and ensures that tickets are handled promptly. Furthermore,

AI enhances ticket routing accuracy by analysing the nature of the issue and directing it to the appropriate department or specialist, thereby minimising delays and improving response and resolution times.

The integration also supports the sustained maintenance of predefined service levels. By automating routine monitoring and reporting tasks, AI ensures that service level agreements (SLAs) are consistently met. This continuous monitoring allows for real-time

adjustments and proactive management, preventing potential breaches of service levels and maintaining high customer satisfaction.

In conclusion, assigning simple, straightforward tasks for automation in IT service desks is highly beneficial. Allowing AI to handle these tasks frees human resources to focus on more complex and strategic issues, enhancing overall operational efficiency. As AI continues to evolve, its role in ITSM systems will likely expand, offering even more significant improvements in service quality and operational effectiveness. “RPA cannot do all the automation, and it needs to be helped in this process by Cognitive Intelligent Automation, Chatbots and Artificial Intelligence” (Anagnoste, 2018).

Infrastructure management

During the early 2000s, infrastructure management was predominantly carried out through manual processes. Server builds necessitated physical CD or DVD drives on physical servers. Network and security features were configured individually, and hardware specifications were tailored to customer requirements for disk space, memory, network, and security. During this period, fundamental skill sets encompassed an understanding of server architecture, basic knowledge of network architecture, and practical hardware proficiency.

In the mid-2000s, a significant change occurred with the introduction of virtualisation. This architecture increased benefits, particularly in server configuration and improved disaster recovery. There were also similar advantages regarding scalability and management, ultimately leading to enhanced cost efficiency.

One of the most notable changes I experienced at this time was the implementation of automation in my professional environment. This allowed us to establish rules, particularly for disaster recovery and configuration. Previously, any failures necessitated a visit to the

data centre, but we could now initiate recovery as soon as possible in most instances of failure. This was my first experience of automation in a real-life enterprise IT scenario. With reduced infrastructure and volume licensing, we had access to the most recent backups and the ability to convert them to production servers rapidly. This transformation also led to a substantial shift in the recruitment landscape, creating a demand for cloud computing skills.

Reflection on IT Infrastructure

During this particular period, I noted a heightened industry awareness of the power consumption of physical servers and their long-term environmental consequences.
Cost savings with power consumption could also be realised. In my professional context, I observed a gradual reduction in the quantity of physical servers in data centres. Additionally, I observed a shift towards increased networked storage in the composition of most company's racks, with a typical outcome being the inclusion of a
The controller server is equipped with some form of storage.
Reflecting on the evolution from traditional physical infrastructure to sophisticated automation in infrastructure management, it becomes apparent that automation has been a transformative force. It has liberated IT professionals from manual monitoring and failure management constraints, enabling us to focus on strategic initiatives that drive business growth and foster innovation.

Automation in Cybersecurity

Integrating automation into IT security encompasses policy implementation, alert prioritisation, incident response planning, threat remediation, continuous monitoring, certificate management, and the development of custom solutions. These automated processes collectively enhance the security posture of organisations by improving efficiency, compliance, and threat response capabilities.
“Automation is becoming a key tool for overwhelmed security personnel as today’s diverse

cyber threats become more widespread, sophisticated, and targeted. Malware, phishing, ransomware, denial-of-service (DoS), zero-day attacks, etc., are common" (Sarker, 2023). Another argument dictates that cyber security as a function will not be able to achieve complete automation, as may be the case with other sub-departments that automation touches.

"The complexity of the task does not allow full automation at this point in time, which causes an ongoing discourse between the need for keeping human operators in the loop despite their physical limitations and the current state of possible automation" (Pawlicka et al., 2021).

Reflection on Automation in Cybersecurity

While automation in IT security offers significant advantages, such as enhanced efficiency, accuracy, and the capacity to manage large data volumes, it is essential to recognise that the complexity of security tasks currently limits the feasibility of complete automation. The ongoing discourse underscores the need for human operators to remain involved despite their physical limitations.

Human oversight is crucial due to the requirement for complex decision-making in many security incidents. Automated systems lack the nuanced judgment and context-awareness that humans bring. Experienced human operators can navigate complex situations with critical thinking that surpasses the capabilities of predefined algorithms.

The continuously evolving landscape of security threats presents another challenge for automated systems. These systems may struggle to adapt to new or unforeseen threats. With their intuition and adaptability, human operators can effectively respond to dynamic environments and emerging security challenges, ensuring a more resilient security posture.

Ethical and moral considerations in security decisions further necessitate human involvement. Some decisions require a moral compass that automated systems cannot provide. Human judgment is vital to ensure that security measures are effective and ethically sound, preventing potentially harmful outcomes without ethical consideration.

Lastly, the need for quality assurance and accountability emphasises the importance of human oversight. Automation can result in false positives or negatives, which could either inundate the system with unnecessary alerts or miss critical threats. Human operators ensure these errors are promptly identified and corrected, maintaining the integrity of security operations. Human involvement establishes a transparent chain of responsibility, ensuring transparency and accountability in security actions.

This further reinforces my earlier observation that human intervention will necessitate the requisite expertise to analyse more intricate reports to identify patterns that may indicate a breach. “Moreover, existing research in host-based detection methods confirms our insight that endpoint monitoring can be used successfully for proactive breach detection” (Bowers & Juels, 2012).

On reflection, while automation greatly enhances IT security, the irreplaceable value of human intervention must not be overlooked. Human operators contribute essential insights, adaptability, and ethical oversight, providing a balanced and reliable security framework. Integrating automation with continuous human monitoring ensures robust and trustworthy security operations.

My conclusion

The future of automation combined with AI in IT service desks, infrastructure management, and cybersecurity is promising, offering substantial efficiency, accuracy, and security improvements. While AI-driven automation will handle routine tasks and provide predictive insights, human oversight will remain essential for complex decision-making, ethical considerations, and ensuring the overall integrity of IT operations. This synergistic approach will lead to more resilient, adaptive, and secure IT environments.

Bibliography

Anagnoste, S. (2018) Robotic Automation Process – The operating system for the digital enterprise. *Proceedings of the International Conference on Business Excellence*, *12*(1), 54–69. https://doi.org/10.2478/PICBE-2018-0007 [Accessed 13 July 2024]

Aslam, F. (2023) The Impact of Artificial Intelligence on Chatbot Technology: A Study on the Current Advancements and Leading Innovations. *European Journal of Technology*, *7*(3), 62–72. https://doi.org/10.47672/EJT.1561 [Accessed 17 July 2024]

Bowers, K. D., & Juels, A. (2012) Research in Attacks, Intrusions, and Defenses. *Research in Attacks, Intrusions and Defenses*, *7462*(2012). [Accessed 14 July 2024]

Kühnel, J., Kühnel, J., Ebner, M., & Ebner, M. (2020) Chatbots for Brand Representation in Comparison with Traditional Websites. In *International Journal of Interactive Mobile Technologies* (Vol. 14, Issue 15). International Association of Online Engineering. https://doi.org/10.3991/ijim.v14i18.13433 [Accessed 12 July 2024]

Martins, I., Andrade, D., & Tumelero, C. (n.d.). (2021) *Increasing customer service efficiency through artificial intelligence chatbot*. https://doi.org/10.1108/REGE-07-2021-0120 [Accessed 17 July 2024]

Pawlicka, A., Pawlicki, M., Kozik, R., & Choraś, R. S. (2021) A Systematic Review of Recommender Systems and Their Applications in Cybersecurity. *Sensors 2021, Vol. 21, Page 5248*, *21*(15), 5248. https://doi.org/10.3390/S21155248 [Accessed 15 July 2024]

Rapp, A., Curti, L., & Boldi, A. (2021) The human side of human-chatbot interaction: A systematic literature review of ten years of research on text-based chatbots. *International Journal of Human Computer Studies*, *151*. https://doi.org/10.1016/j.ijhcs.2021.102630 [Accessed 12 July 2024]

Samarakoon, L., Kumarawadu, S., & Pulasinghe, K. (2011) Automated question answering for customer helpdesk applications. *2011 6th International Conference on Industrial and Information Systems, ICIIS 2011 - Conference Proceedings*, 328–333. https://doi.org/10.1109/ICIINFS.2011.6038089 [Accessed 15 July 2024]

Sarker, I. H. (2023) Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. *Annals of Data Science*, *10*(6), 1473–1498. https://doi.org/10.1007/S40745-022-00444-2/FIGURES/6 [Accessed 14 July 2024]

Zangari, A., Marcuzzo, M., Schiavinato, M., Gasparetto, A., & Albarelli, A. (2023) Ticket automation: An insight into current research with applications to multi-level classification scenarios. *Expert Systems with Applications*, *225*, 119984. https://doi.org/10.1016/J.ESWA.2023.119984 [Accessed 14 July 2024]