Campus AI vs Commercial AI: A Late-Breaking Study on How LLM As-A-Service Customizations Shape Trust and Usage Patterns

LEON HANNIG, University of Duisburg-Essen, Germany

ANNIKA BUSH, TU Dortmund University, Germany

MELTEM AKSOY, TU Dortmund University, Germany

STEFFEN BECKER*, Ruhr University Bochum, Germany

GRETA ONTRUP, University of Duisburg-Essen, Germany

As the use of Large Language Models (LLMs) by students, lecturers and researchers becomes more prevalent, universities – like other organizations – are pressed to develop coherent AI strategies. LLMs as-a-Service (LLMaaS) offer accessible pre-trained models, customizable to specific (business) needs. While most studies prioritize data, model, or infrastructure adaptations (e.g., model fine-tuning), we focus on user-salient customizations, like interface changes and corporate branding, which we argue influence users' trust and usage patterns. This study serves as a functional prequel to a large-scale field study in which we examine how students and employees at a German university perceive and use their institution's customized LLMaaS compared to ChatGPT. The goals of this prequel are to stimulate discussions on psychological effects of LLMaaS customizations and refine our research approach through feedback. Our forthcoming findings will deepen the understanding of trust dynamics in LLMs, providing practical guidance for organizations considering LLMaaS deployment.

1 Introduction

As Large Language Models (LLMs) become increasingly prevalent in professional and educational settings, organizations face mounting pressure to develop coherent strategies for AI integration [32]. Current research shows high adoption rates of commercial off-the-shelf LLMs such as ChatGPT among students and university staff for various professional and academic tasks [59, 65, 66]. In order to guide the informed and secure use of AI, many organizations, including universities, corporations, and government agencies, are exploring the deployment of LLMs as-a-Service (LLMaaS) as an achievable and cost-effective way to adopt AI in-house [33]. This trend is driven by several practical considerations: the opportunity to offer access to all university members while maintaining institutional oversight and alignment with organizational policies or the ability to provide dedicated technical support [46]. One of the main benefits of AI as-a-Service (AIaaS) solutions is the flexibility they offer in customizing various aspects [22], such as fine-tuning models or displaying user interfaces in corporate design.

Customizations are important because they can, e.g., improve model performance for the specific organizational context or enhance security and privacy safeguards [35, 55]. However, even choices that do not impact model performance or security, such as branding a user interface, could lead to significant changes in how the system is perceived and used.

---

*Also with Max Planck Institute for Security and Privacy.

Authors' Contact Information: Leon Hannig, University of Duisburg-Essen, Duisburg, Germany, leon.hannig@uni-due.de; Annika Bush, TU Dortmund University, Dortmund, Germany, annika.bush@tu-dortmund.de; Meltem Aksoy, TU Dortmund University, Dortmund, Germany, meltem.aksoy@tu-dortmund.de; Steffen Becker, Ruhr University Bochum, Bochum, Germany, steffen.becker@rub.de; Greta Ontrup, University of Duisburg-Essen, Duisburg, Germany, greta.ontrup@uni-due.de.

From a psychological perspective, users rely on various cues to assess the trustworthiness and consequently align their use of AI [21, 53]. Users interpret information about and from the system in terms of its performance, purpose, and processes [21]. We argue that end users may interpret customizations of LLMs as indicative of the system's capabilities, goals, and underlying processes, even if the design choices (e.g., corporate branding) do not directly impact functionality.

While organizations invest in LLMaaS, we lack systematic empirical evidence on how customization choices within the adoption process influence users' trust, usage patterns, and overall acceptance of these systems compared to commercial off-the-shelf alternatives (hereinafter referred to as "commercial LLMs"). This is especially relevant for customization choices that are salient to the user (e.g., user interface) but have no real technical impact on the pre-trained data/model/algorithm/infrastructure [22]. We aim to close this research gap by conducting an empirical study that answers the following research question:

> **RQ:** How do customizations of LLMaaS impact end users' trust, perception, and usage of LLMs in professional and academic contexts compared to commercial AI alternatives?

This late-breaking work presents the research motivation, hypotheses, and study design of an ongoing large-scale field study. The purpose of this "prequel" is twofold: first, we compile a comprehensive overview of LLMaaS customization options to guide the hypothesis formulation, aiming to stimulate further discussion and research into the psychological effects of customization choices on end users. Second, we seek feedback from our professional peers on our proposed field study to enhance its effectiveness. Outcomes from our large-scale field study will enrich both theoretical insights into trust in organizational AI systems and practical applications of AI strategies across different sectors.

2 Background

2.1 LLMs (as-a-Service) at Universities

LLMs, such as ChatGPT, have become increasingly prevalent in academic settings, with significant adoption among university students. For example, von Garrel and Mayer [59] report that nearly two thirds of German students use LLMs for tasks that include concept clarification, literature review, and translation. Similarly, Amani et al. [5] demonstrate the widespread use of LLMs for personalized learning purposes at Texas A&M University. Researchers have reported using LLMs [32, 56], e.g., for language editing or literature search [2].

Thus, universities are caught between enabling students and staff to access and use AI in an informed way to leverage the benefits while also protecting data, privacy, rights, and ethical principles. One way to appropriately shape the use of AI is for universities to introduce "their own" LLMs, the same way as organizations in the private sector do (e.g., WärtsiläGPT by the Finnish company Wärtsilä Oyi; [46]). However, the introduction of AI poses a massive challenge for universities, due to a lack of internal technical abilities and knowledge about the deployment of AI and the high costs of developing and maintaining a sufficient IT infrastructure [36].

LLMs as-a-Service (LLMaaS) provide a practical solution by offering easy access to pre-trained models via cloud providers [61]. This approach is a subset of AI as-a-Service (AIaaS), broadly defined as "cloud-based systems providing on-demand services to organizations and individuals for deploying, developing, training, and managing AI models" [36, p. 424]. Often referred to as "no-code or low-code" AI, these systems are recognized as a means of democratizing AI, enabling organizations to adopt and afford AI technologies without requiring extensive technological expertise [55]. Moreover, LLMaaS solutions emphasize enhanced data protection and security, offering a viable option for institutions like universities to leverage AI's advantages while adhering to stringent compliance and security standards [46]. The primary benefits of AIaaS include reducing complexity, increasing automation, and enabling customization [36].

One proposed advantage of LLMaaS is that organizations can tailor various aspects of LLMs to better align with their unique requirements and objectives. In this context, customizations are defined as configurations of parameters at various architectural layers to improve the fit between the system and organization-specific needs [22]. Table 1 outlines customization options, which encompass customizations of data, models, algorithms, and infrastructure [22], security and governance adaptations [15], customizations that relate to the design of the user interface and experience, and choices regarding the organizational integration.

Table 1. Examples of Customization Aspects of AIaaS.

Category	Examples	References
Model fine-tuning and Configuration	Adjust/add system prompts, fine-tuning on proprietary data, hyper-parameter configuration, domain-specific knowledge integration, customizable output.	[22, 26, 33, 36, 47]
Integration and Interoperability	API integration, integration with other tools and systems.	[24, 36]
Security and Governance	Access control and security, compliance and regulatory requirements, monitoring and evaluation.	[23, 24, 30, 47]
User Interface and Experience	Incorporation of corporate design, sustainability measures (e.g., token visualization), user profiling and personalization, customizable error handling, multi-language support.	[13]
Organizational integration	Providing context-specific training or workshops, providing context-specific information and use recommendations regarding the model.	[42]

To date, existing literature has focused primarily on methods and effects of model fine-tuning and configuration, integration and interoperability, as well as security and governance-related consequences of LLMaaS. These aspects are critical, as adapting AI systems – for example, to ensure data protection or to fine-tune them for internal company data – plays a key role in their secure and human-centered integration into organizations. However, other customization choices, such as interface design, remain largely unexplored in terms of their impact on end users. For instance, research and reports on LLMaaS deployment in organizations focus mostly on technical customizations, mentioning other customizations pertaining to the user interface and experience or the organizational integration as a side note (e.g., Weber et al. [62] report on the architectural designs of Frauenhofers LLMaaS "FhGenie"). This could be because these adjustments have no effect on the actual performance or security of the models. However, from a psychological perspective, users' trust and corresponding use of AI depend on so-called cues, i.e. "any information element that can be used to make a trust assessment about an agent" [21, p. 253]. Users have been shown to rely on various cues when deciding whether or not to trust and use AI, e.g., system explanations or a logo of a company [53]. Gong et al. [25] for example theorize on the effects of user experience (UX) design on perceived trustworthiness. We therefore posit that it is essential to recognize that end users could perceive customizations of LLMs as reflections of the system's capabilities, goals, and inner workings, even if these customizations (such as using a corporate design) do not actually affect the functioning of the system.

This study investigates the usage patterns and trust perceptions of end users when interacting with commercial LLMs and customized LLMaaS. In the following, we derive hypotheses based on previous research to assess how the customization choices of LLMaaS affect the perception and use of the system by users compared to a commercial LLM.

2.2 Trust in AI Systems

Trust, as a key determinant of technology adoption [17, 58], has been recognized as an important factor for LLM adoption among academic staff and students [9, 57]. Research has shown that both insufficient and excessive trust in AI systems can be critical, as a lack of trust may hinder their adoption, while overtrust can lead to risks such as reliance on incorrect or potentially harmful outputs [11, 60]. This underscores the importance of ensuring that students and staff place appropriate trust in LLM chatbots.

Trust is commonly defined as the trustor's positive expectations towards the trustee, combined with the trustor's vulnerability and uncertainty within the specific context [7, 34]. Research has shown that trust levels in human-human interaction depend on three perceived qualities of the trustee: ability, integrity, and benevolence [38]. In the context of human-automation interaction, these three factors have been reframed as performance, process (e.g. availability, confidentiality, understandability of a system) and purpose (e.g., the developer's intentions) [34]. Additional factors have been identified as particularly important for trust in LLMs. These include transparency [29, 54], access to a human operator [44], and perceived privacy and robust data security [29, 48]. These insights provide a robust basis for examining how users develop trust when choosing between organizations' customized LLMaaS and commercial LLMs.

Customizations of LLMaaS in corporate design could serve as a salient trust cue for users, increasing the perceived trustworthiness of the system in two dimensions: (a) purpose and (b) process. The perceived purpose of the system may appear more trustworthy when the customizations incorporate university branding, as the university is likely to be seen as a benevolent provider with minimal financial or marketing-driven motives [44]. This perception may be further enhanced due to a sense of familiarity evoked by the university's branding [3]. Second, the process dimension of the system may be perceived as more trustworthy because it is easily accessible and embedded in the existing organizational framework. Here, features such as the option to contact a human operator for assistance could contribute to users' trust through perceived openness and accessibility [34]. Additionally, a customized LLMaaS may be perceived as more transparent due to context-specific information about the system available on the university's website. These factors together lead us to the following hypothesis:

> **H1:** Users report higher levels of trust in a customized LLMaaS compared to a commercial LLM.

We further hypothesize that higher trust in the organization's customized LLMaaS will likely depend on its members' trust in the organization itself. Organizational trust describes the extent to which individuals trust an organization [50]. Prior research on AI implementation [67] and attitudes towards LLMs [7] suggests that organizational trust can significantly shape users' trust in the system. In line with this, Nordheim et al. [44] have demonstrated that customers' trust in a company's service chatbot is influenced by their trust in the company itself. We therefore assume:

> **H2:** The level of organizational trust moderates the effect of system type (customized vs. commercial) on user trust, such that the effect is stronger when organizational trust is higher and weaker when it is lower.

2.3 LLM Hallucinations

When implementing LLMaaS, universities face the challenge of ensuring that their students and staff can interact with these systems effectively, correctly and safely. A key aspect of this responsibility is addressing the issue of hallucinations. Hallucinations in LLMs describe the generation of content that appears plausible but is either factually

incorrect or inconsistent with user input [28]. Hallucinations in human-AI interaction pose a dual challenge: they impair effective collaboration through reduced output quality and undermine users' trust [25, 45]. In the academic context, hallucinations present particularly serious risks. For example, LLMs have been shown to often fabricate inaccurate scientific references [4, 14]. For university staff and students, hallucinations could thus lead to severe consequences.

Despite various efforts and technological advances, hallucinations cannot be completely eliminated from LLMs [8, 64]. This issue calls for a focus on the human side, with the ultimate goal of identifying strategies to help users anticipate, mitigate, and react to hallucinations. In this context, we consider two customization aspects of the user interface: corporate design and warnings about false information. Research has shown that the presence of logos from reputable companies can create positive associations, enhancing the perceived credibility of mobile systems [37]. We argue that branding a chatbot with a university logo leads users to interpret the chatbot as university-approved, i.e., reliable and infallible. This could potentially make users less critical and cautious in their interactions with the university-branded system. Another notable customization choice of LLMaaS is the display of warnings about hallucinations or false information. Research suggests that such warnings can help users detect hallucinations more frequently [43]. While ChatGPT's interface includes a disclaimer below the prompt box stating "ChatGPT can make mistakes. Please consider checking important information", LLMaaS allow such warnings to be adapted, removed, or altered. We argue that making hallucination warnings less visible leads users to be less cautious about hallucinations in their LLM interactions, and thus to detect fewer hallucinations. Based on this reasoning, we propose the following hypotheses:

> **H3:** Users report less cautious behavior towards hallucinations when using a customized LLMaaS compared to a commercial LLM.

> **H4:** Users report fewer experienced hallucinations when using a customized LLMaaS compared to a commercial LLM.

2.4 Data Security and Privacy Concerns

End users often express concerns about data security and privacy when interacting with LLMs. Key risks include (unauthorized) data retention [19], where providers may retain and use customer data to enhance their models, inference attacks that aim to extract sensitive information from trained models [31], and the unintended exposure of confidential data during model training or operation [16]. Technical customization options in LLMaaS offer promising avenues to mitigate these risks, thereby playing a pivotal role in enhancing users' perceptions of privacy and security while fostering trust. These options include user-configurable privacy settings that empower users to control how their data is stored and used [6], transparency mechanisms like privacy explanations [10], which provide clarity about data handling practices, and the implementation of privacy-preserving techniques such as differential privacy [1] during training and fine-tuning processes. Beyond their direct technical benefits, we posit that customization measures, even those without tangible impacts on privacy or security, can still foster higher perceived privacy levels. In this context, we again draw on the role of corporate branding as a salient customization feature: institution-branded LLMs could enhance data security and privacy perceptions, which in turn could lead users to perceive the system as more trustworthy, believing that their data will be handled with care and not shared with third parties. In this context, we propose the following hypothesis:

> **H5:** Users perceive greater privacy when using a customized LLMaaS compared to a commercial LLM.

2.5 Sustainable AI Use

Having explored potential impacts of customization on users' trust, perceived hallucinations and privacy concerns, it becomes evident that organizations need to carefully consider their approach to LMMaaS. In this last part, we want to

open the door for broader considerations that pertain to the global strategy of an organization, specifically the corporate social responsibility (CSR). CSR refers to situations in which organizations pursue strategies that go beyond business needs and legal regulations but aim at furthering social good [40]. This includes various aspects, such as improving an organization's sustainability and environmental performance [41]. We argue that customization of LLMaaS offer organizations opportunities to align AI deployment with their CSR strategy and corresponding sustainability goals, thereby not only shaping the trust in and perception of the systems but also their environmental impact.

The environmental impact of AI systems and LLMs has become an increasingly critical concern in computing research. Recent work by Rafael and Reis [51] emphasizes how the invisibility of digital energy consumption often leads to unconscious and potentially wasteful usage patterns. This mirrors findings in energy consumption studies [39] that identify varying levels of user awareness – from "energy unaware" to "energy aware and active" – highlighting how visibility of resource consumption can transform user behavior. Our research extends these insights and considers the impact of customization choices aimed at promoting sustainable AI usage patterns.

Making resource consumption visible has shown promising results across different domains. Penkert and Gröschel [49] demonstrated that transparency in sustainability information significantly influences user choices, while Sanduleac et al. [52] found that real-time energy data promotes more responsible consumption patterns. LLMaaS offer customization options to make AI resource limitations explicit through token visibility. We argue that customizing token visibility can foster what we term "AI resource consciousness" – a more deliberate and efficient approach to AI interaction that considers both immediate utility and broader environmental impact. Based on these previous findings, we hypothesize:

> **H6:** Users report (a) more resource-efficient prompting behaviors and (b) increased sensitivity to AI sustainability concerns when using a customized LLMaaS compared to a commercial LLM.

3 Method

3.1 Study Design, Participants and Setting

To answer our hypotheses, we plan a quantitative, cross-sectional field study. We designed a comprehensive survey instrument combining validated measures from existing research with questions specific to the use of LLM-based chatbots. In the following, we report on the planned design, method and questionnaire.

The large-scale study will be conducted in the spring of 2025 at a large German research university that has implemented a customized LLMaaS in late 2024. The system has approximately 6,000 registered users and 800 active users per week as of January 22, 2025. Our participant pool includes three distinct user groups within the university ecosystem: (a) students across all academic levels and disciplines, (b) research staff, including PhDs, PostDocs, faculty, and (c) administrative staff. A sample size of $N = 250$ (accounting for dropout) is planned ($f^2 = 0.05$, $\alpha = 0.05$, $\beta = .80$). The goal is to ensure an equal distribution of participants between users of the customized LLMaaS and ChatGPT as well as an equal representation across the three status groups.

3.2 Customized LLMaaS

The LLM-based chatbot introduced by the university is OpenAI's ChatGPT deployed via Microsoft Azure. Customizations regarding the data and model were kept to a minimum, but the university made some adjustments regarding the user interface and incorporated detailed information and training materials (see Table 2).

Table 2. Customization features of the studied LLMaaS.

Category	Customization Details
Model fine-tuning & Configuration	Temperature[1] set to 0 for deterministic outputs
Integration and Interoperability	Access to multiple models; image generation via DALL-E for OpenAI models
Security and Governance	Minimal data collection for service provision; chat data excluded from model training; GDPR-compliant data processing within the EU; access restricted to internal networks (e.g., via VPN)
User Interface and Experience	Interface customized with corporate design (e.g., university logo); token usage visualized as a percentage in the user interface
Organizational integration	Supporting materials provided on the chatbot landing page and intranet; training sessions on effectively using LLMs in higher education

[1] The temperature parameter in LLMs, ranging from 0 to 1, controls response randomness, with values near 0 favoring deterministic outputs and values near 1 producing diverse, creative outputs.

3.3 Survey Instrument

We designed a comprehensive survey to investigate the perceptions and usage patterns of both the university's customized LLMaaS chatbot and OpenAI's ChatGPT. The proposed survey design is summarized in Figure 1. Participants are guided through the survey based on their use/non-use of the university-customized chatbot and ChatGPT. The main part consists of questions regarding the perception and use of the university's system and ChatGPT (green blocks in Figure 1). The survey questions are available in the supplementary material.
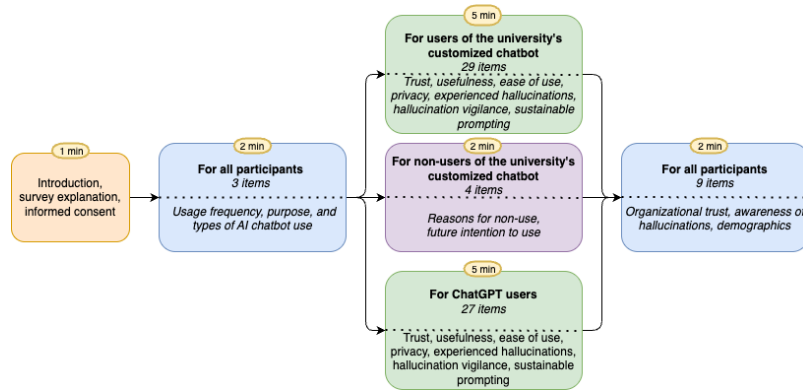

Fig. 1. Overview of our survey. The expected completion time is 15 minutes or less.

The survey begins by capturing usage patterns, including frequency of use (ranging from "never" to "multiple times per day") and the context of use (private versus work/study-related). In the first step, several aspects of system perception and use are explored: the context of use (specific tasks), use of training/information material, perceived usefulness (productivity enhancement, task facilitation), and ease of use (interface clarity, learning curve), both assessed following the Technology Acceptance Model (TAM)[20]. For users familiar with either system, we also assess their awareness and use of different language models available within each platform. For users who have never used or rarely use the university's chatbot, we explore their reasons for non-adoption or limited use.

The main part of the survey is structured around the key constructs (see hypotheses), measured in parallel for both systems. Participants who use both systems will respond to the same set of items twice: once for the university's customized LLMaaS and once for ChatGPT. At the beginning of the main part, participants are reminded to answer the following questions specifically in regard to their work-related or academic use of the chatbots, and not for their private use. We use five-point Likert scales ranging from "strongly disagree" to "fully agree".

Trust. Trust is measured along two dimensions: trust in the providing organization (university) is measured with three items following Bøe [12] (e.g., "My university will safeguard my interests.") and trust in the chatbots themselves is assessed by the facets of global trust, benevolence/purpose, integrity/process and ability/performance using four items from Wischnewski et al. [63] (e.g., "I trust [the university's chatbot/ChatGPT].").

Hallucinations. We investigate users' cautious behavior towards LLM hallucinations, including their verification practices and task-specific trust decisions, with three items (e.g., "I check important information from [the university's chatbot/ChatGPT] responses through external sources."). Users also report their experienced hallucinations with three items (e.g., "I have noticed that [the university's chatbot/ChatGPT] makes up facts that do not correspond to reality."). The items are self-developed based on Christensen et al. [18].

Data security and privacy concerns. We measure privacy concerns following Hsu and Lin [27] with three items (e.g., "My decision to use [the university's chatbot/ChatGPT] exposes me to privacy risks.").

Sustainable AI use. The survey also assesses the intentions for sustainable use, environmentally conscious behavior, and considerations of energy consumption with three items (e.g., "I often think about the energy consumption of [the university's chatbot/ChatGPT]."). Since the university-chatbot displays the remaining number of tokens as a percentage, we assessed the university-chatbot users' awareness of token usage with two items (e.g., "During use, I pay attention to how many tokens I still have available."). Because there are no tested surveys focusing explicitly on the sustainable use of LLMs yet, the items are self-developed.

3.4   Data Collection Procedure

To maximize participation and ensure representative sampling, we employ a multi-channel recruitment strategy through the university's chatbot landing page, department office communications, university-wide communication channels, and supplementary physical materials where needed. The university communications department will assist in disseminating the survey through official social media channels and website postings.

4   Outlook: Expected Contributions

Our research provides three key contributions to the field: First, for higher education institutions and organizations in general, we offer evidence-based insights for AI implementation strategies, helping decision-makers understand how customization choices of LLMaaS solutions impact user trust and adoption patterns. Second, we develop design recommendations for organizational AI systems, addressing how features, interfaces, and integration approaches can be optimized to enhance user trust and adoption while effectively coexisting with commercial alternatives. Third, we open new research directions for investigating how customization aspects, especially organizational AI branding effects, vary across sectors, examining long-term impacts on organizational culture, and exploring the evolving relationship between institutional trust and AI system trust over time.

Acknowledgments

References

[1] Martin Abadi, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar, and Li Zhang. 2016. Deep Learning with Differential Privacy. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery, New York, NY, USA, 308–318.

[2] A. S. Abdelhafiz, A. Ali, A. M. Maaly, H. H. Ziady, E. A. Sultan, and M. A. Mahgoub. 2024. Knowledge, Perceptions and Attitude of Researchers Towards Using ChatGPT in Research. *Journal of Medical Systems* 48, 1 (Feb 2024), 26. doi:10.1007/s10916-024-02044-4

[3] Gene M. Alarcon, Joseph B. Lyons, and James C. Christensen. 2016. The effect of propensity to trust and familiarity on perceptions of trustworthiness over time. *Personality and Individual Differences* 94 (2016), 309–315. doi:10.1016/j.paid.2016.01.031

[4] Fahad Aljamaan, Majed Temsah, Ibrahim Altamimi, Abdulrahman Al-Eyadhy, Ammar Jamal, Khalid Alhasan, Tariq Mesallam, Mohammed Farahat, and Khalid Malki. 2024. Reference Hallucination Score for Medical Artificial Intelligence Chatbots: Development and Usability Study. *JMIR Medical Informatics* 12 (2024), e54345. doi:10.2196/54345

[5] S. Amani, L. White, T. Balart, L. Arora, K. J. Shryock, K. Brumbelow, and K. L. Watson. 2023. Generative AI Perceptions: A Survey to Measure the Perceptions of Faculty, Staff, and Students on Generative AI Tools in Academia. *ArXiv* (2023). https://arxiv.org/abs/2304.14415 arXiv preprint.

[6] Paul Ashley, Satoshi Hada, Günter Karjoth, and Matthias Schunter. 2002. E-P3P privacy policies and privacy authorization. In *Proceedings of the 2002 ACM Workshop on Privacy in the Electronic Society* (Washington, DC) *(WPES '02)*. Association for Computing Machinery, New York, NY, USA, 103–109. doi:10.1145/644527.644538

[7] Agathe Balayn, Mireia Yurrita, Fanny Rancourt, Fabio Casati, and Ujwal Gadiraju. 2024. An Empirical Exploration of Trust Dynamics in LLM Supply Chains. arXiv:2405.16310 [cs.HC] https://arxiv.org/abs/2405.16310

[8] Sourav Banerjee, Ayushi Agarwal, and Saloni Singla. 2024. LLMs Will Always Hallucinate, and We Need to Live With This. arXiv:2409.05746 [stat.ML] https://arxiv.org/abs/2409.05746

[9] P. Bhaskar, P. Misra, and G. Chopra. 2024. Shall I use ChatGPT? A study on perceived trust and perceived risk towards ChatGPT usage by teachers at higher education institutions. *International Journal of Information and Learning Technology* 41, 4 (2024), 428–447. doi:10.1108/IJILT-11-2023-0220

[10] Wasja Brunotte, Alexander Specht, Larissa Chazette, and Kurt Schneider. 2023. Privacy explanations – A means to end-user trust. *Journal of Systems and Software* 195 (2023), 111545. doi:10.1016/j.jss.2022.111545

[11] Zana Buçinca, Maja Barbara Malaya, and Krzysztof Z. Gajos. 2021. To Trust or to Think: Cognitive Forcing Functions Can Reduce Overreliance on AI in AI-assisted Decision-making. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW1, Article 188 (April 2021), 21 pages. doi:10.1145/3449287

[12] Tove Bøe. 2018. E-learning technology and higher education: the impact of organizational trust. *Tertiary Education and Management* 24, 4 (2018), 362–376. doi:10.1080/13583883.2018.1465991 arXiv:https://doi.org/10.1080/13583883.2018.1465991

[13] Fabio Casati, Kannan Govindarajan, Baskar Jayaraman, Aniruddha Thakur, Sriram Palapudi, Firat Karakusoglu, and Debu Chatterjee. 2019. Operating Enterprise AI as a Service. In *Service-Oriented Computing. ICSOC 2019. Lecture Notes in Computer Science*, Slimane Yangui, Ines Bouassida Rodriguez, Khalil Drira, and Zahir Tari (Eds.). Vol. 11895. Springer, Cham. doi:10.1007/978-3-030-33702-5_25

[14] Mikaël Chelli, Jules Descamps, Vincent Lavoué, Christophe Trojani, Michel Azar, Marcel Deckert, Jean-Luc Raynier, Gilles Clowez, Pascal Boileau, and Caroline Ruetsch-Chelli. 2024. Hallucination Rates and Reference Accuracy of ChatGPT and Bard for Systematic Reviews: Comparative Analysis. *J Med Internet Res* 26 (22 May 2024), e53164. doi:10.2196/53164

[15] M. Chen, C. Xiao, H. Sun, L. Li, L. Derczynski, A. Anandkumar, and F. Wang. 2024. Combating Security and Privacy Issues. In *Human Language Technologies*, Y. Cao, I. Papadimitriou, A. Ovalle, M. Zampieri, F. Ferraro, and S. Swayamdipta (Eds.). Association for Computational Linguistics, Mexico City, Mexico, 16–21. Symposium conducted at the meeting of Association for Computational Linguistics.

[16] Xiaoyi Chen, Siyuan Tang, Rui Zhu, Shijun Yan, Lei Jin, Zihao Wang, Liya Su, Zhikun Zhang, XiaoFeng Wang, and Haixu Tang. 2024. The Janus Interface: How Fine-Tuning in Large Language Models Amplifies the Privacy Risks. In *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security* (Salt Lake City, UT, USA) *(CCS '24)*. Association for Computing Machinery, New York, NY, USA, 1285–1299. doi:10.1145/3658644.3690325

[17] Avishek Choudhury and Hamid Shamszare. 2023. Investigating the Impact of User Trust on the Adoption and Use of ChatGPT: Survey Analysis. *J Med Internet Res* 25 (14 Jun 2023), e47184. doi:10.2196/47184

[18] Jeff Christensen, Jared M. Hansen, and Paul Wilson. 2024. Understanding the role and impact of Generative Artificial Intelligence (AI) hallucination within consumers' tourism decision-making processes. *Current Issues in Tourism* 0, 0 (2024), 1–16. doi:10.1080/13683500.2023.2300032 arXiv:https://doi.org/10.1080/13683500.2023.2300032

[19] Jennifer Cobbe and Jatinder Singh. 2021. Artificial intelligence as a service: Legal responsibilities, liabilities, and policy challenges. *Computer Law & Security Review* 42 (2021), 105573. doi:10.1016/j.clsr.2021.105573

[20] Fred D Davis. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly* (1989), 319–340.

[21] E. J. de Visser, M. Cohen, A. Freedy, and R. Parasuraman. 2014. A Design Methodology for Trust Cue Calibration in Cognitive Agents. In *Virtual, Augmented and Mixed Reality. Designing and Developing Virtual and Augmented Environments*, R. Shumaker and S. Lackey (Eds.). Lecture Notes in Computer Science, Vol. 8525. Springer, Cham, 194–204. doi:10.1007/978-3-319-07458-0_24

[22] Lorenzo Diaferia, Ivo Blohm, Leonardo Maria De Rossi, and Gianluca Salviotti. 2022. When Standard Is Not Enough: A Conceptualization of AI Systems' Customization and its Antecedents. In *ICIS 2022 Proceedings*. 8. https://aisel.aisnet.org/icis2022/is_implement/is_implement/8

[23] A. Doosthosseini, J. Decker, H. Nolte, and J. M. Kunkel. 2024. Chat AI: A Seamless Slurm-Native Solution for HPC-Based Services. ArXiv. https://arxiv.org/abs/2407.00110

[24] W. Gan, S. Wan, and P. S. Yu. 2023. Model-as-a-Service (MaaS): A Survey. arXiv:2311.05804 [cs.CL] https://arxiv.org/abs/2311.05804

[25] Zhiyun Gong, Shivani Birajdar, Tam Cao, Yi Qing Khoo, Chia-Fang Chung, Yassi Moghaddam, Anbang Xu, Hridhay Mehta, Aaditya Shukla, Zhilin Wang, et al. 2024. Enhancing Trust in LLM Chatbots for Workplace Support Through User Experience Design and Prompt Engineering. *The Human Side of Service Engineering* (2024), 139.

[26] Valiollah Hajipour, Saeid Hekmat, and Mehdi Amini. 2023. A value-oriented Artificial Intelligence-as-a-Service business plan using integrated tools and services. *Decision Analytics Journal* 8 (2023), 100302. doi:10.1016/j.dajour.2023.100302

[27] Chin-Lung Hsu and Judy Chuan-Chuan Lin. 2018. Exploring Factors Affecting the Adoption of Internet of Things Services. *Journal of Computer Information Systems* 58, 1 (2018), 49–57. doi:10.1080/08874417.2016.1186524

[28] Lei Huang, Weijiang Yu, Weitao Ma, Weihong Zhong, Zhangyin Feng, Haotian Wang, Qianglong Chen, Weihua Peng, Xiaocheng Feng, Bing Qin, and Ting Liu. 2024. A Survey on Hallucination in Large Language Models: Principles, Taxonomy, Challenges, and Open Questions. *ACM Transactions on Information Systems* (Nov. 2024). doi:10.1145/3703155

[29] Yue Huang, Qihui Zhang, Philip S. Y, and Lichao Sun. 2023. TrustGPT: A Benchmark for Trustworthy and Responsible Large Language Models. arXiv:2306.11507 [cs.CL] https://arxiv.org/abs/2306.11507

[30] U. Iqbal, T. Kohno, and F. Roesner. 2024. LLM Platform Security: Applying a Systematic Evaluation Framework to OpenAI's ChatGPT Plugins. In *AAAI/ACM Conference on AI, Ethics, and Society (AIES-24)*, S. Das, B. P. Green, K. Varshney, M. Ganapini, and A. Renda (Eds.). arXiv, 611–623. doi:10.1609/aies.v7i1.31664

[31] Nikhil Kandpal, Krishna Pillutla, Alina Oprea, Peter Kairouz, Christopher A. Choquette-Choo, and Zheng Xu. 2024. User Inference Attacks on Large Language Models. In *Proceedings of the 2024 Conference on Empirical Methods in Natural Language Processing*, Yaser Al-Onaizan, Mohit Bansal, and Yun-Nung Chen (Eds.). Association for Computational Linguistics, Miami, Florida, USA, 18238–18265. doi:10.18653/v1/2024.emnlp-main.1014

[32] S. Kapania, R. Wang, T. J. Li, T. Li, and H. Shen. 2024. "I'm categorizing LLM as a productivity tool": Examining ethics of LLM use in HCI research practices. arXiv:2403.19876 [cs.HC] https://arxiv.org/abs/2403.19876

[33] E. La Malfa, A. Petrov, S. Frieder, C. Weinhuber, R. Burnell, R. Nazar, A. G. Cohn, N. Shadbolt, and M. Wooldridge. 2023. Language Models as a Service: Overview of a New Paradigm and its Challenges. arXiv:2309.16573 [cs.CL] https://arxiv.org/abs/2309.16573

[34] John D Lee and Katrina A See. 2004. Trust in automation: Designing for appropriate reliance. *Human factors* 46, 1 (2004), 50–80.

[35] K. Lewicki, M. S. Lee, J. Cobbe, and J. Singh. 2023. Out of Context: Investigating the Bias and Fairness Concerns of "Artificial Intelligence as a Service". ArXiv. doi:10.1145/3544548.3581463

[36] S. Lins, K. D. Pandl, H. Teigeler, et al. 2021. Artificial Intelligence as a Service. *Business & Information Systems Engineering* 63 (2021), 441–456. doi:10.1007/s12599-021-00708-w

[37] Paul Benjamin Lowry, Tom Roberts, and Bryce Eryn Caine. 2005. The effect of familiar logos on trust of websites designed for small user interfaces. In *11th International Conference on Human-Computer Interaction (HCII 2005), Las Vegas, Nevada, July, Citeseer*. 22–27.

[38] RC Mayer. 1995. An Integrative Model of Organizational Trust. *Academy of Management Review* (1995).

[39] Stephen McCarthy, Titiana Ertiö, Ciara Fitzgerald, and Nina Kahma. 2023. Sustainable Energy Behaviors through Green Information Systems: An Exploratory Study. In *2023 IEEE International Symposium on Technology and Society (ISTAS)*. IEEE, 1–8. doi:10.1109/ISTAS57930.2023.10306166

[40] A. McWilliams and D. Siegel. 2001. Corporate Social Responsibility: a Theory of the Firm Perspective. *Academy of Management Review* 26, 1 (2001), 117–127. doi:10.5465/amr.2001.4011987

[41] A. McWilliams, D.S. Siegel, and P.M. Wright. 2006. Corporate Social Responsibility: Strategic Implications. *Journal of Management Studies* 43, 1 (2006), 1–18. doi:10.1111/j.1467-6486.2006.00580.x

[42] R. Nagarajan, M. Kondo, F. Salas, E. Sezgin, Y. Yao, V. Klotzman, S. A. Godambe, N. Khan, A. Limon, G. Stephenson, S. Taraman, N. Walton, L. Ehwerhemuepha, J. Pandit, D. Pandita, M. Weiss, C. Golden, A. Gold, J. Henderson, A. Shippy, L. A. Celi, W. R. Hogan, E. K. Oermann, T. Sanger, and S. Martel. 2024. Economics and Equity of Large Language Models: Health Care Perspective. *J Med Internet Res* 26 (2024), e64226. doi:10.2196/64226

[43] Mahjabin Nahar, Haeseung Seo, Eun-Ju Lee, Aiping Xiong, and Dongwon Lee. 2024. Fakes of Varying Shades: How Warning Affects Human Perception and Engagement Regarding LLM Hallucinations. arXiv:2404.03745 [cs.HC] https://arxiv.org/abs/2404.03745

[44] Cecilie Bertinussen Nordheim, Asbjørn Følstad, and Cato Alexander Bjørkli. 2019. An initial model of trust in chatbots for customer service—findings from a questionnaire study. *Interacting with Computers* 31, 3 (2019), 317–335. doi:10.1093/iwc/iwz022

[45] R. Oelschlager. 2024. *Evaluating the Impact of Hallucinations on User Trust and Satisfaction in LLM-based Systems*. Dissertation. Linnaeus University. https://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-130539 Retrieved from https://urn.kb.se/resolve?urn=urn:nbn:se:lnu:diva-130539.

[46] Ira Aurora Paavola. 2024. *Evaluating Generative AI Literacy among HR Personnel to Develop a Framework for an Internal GPT*. Master's Thesis. Tampere University, Faculty of Information Technology and Communication Sciences. https://example.com/your-thesis-url

[47] V.B. Parthasarathy, A. Zafar, A. Khan, and A. Shahid. 2024. *The Ultimate Guide to Fine-Tuning LLMs from Basics to Breakthroughs: An Exhaustive Review of Technologies, Research, Best Practices, Applied Research Challenges and Opportunities.* CeADAR Connect Group.

[48] Marta Pawłowska-Nowak. 2024. Identification of Trust Determinants in LLM Technology Using the DEMATEL Method. *European Research Studies Journal* 27, S2 (2024), 694–711.

[49] Lydia Penkert and Carla Gröschel. 2023. Increasing sustainable user behavior in digital products through transparent sustainability information. In *Mensch und Computer 2023*, Markus Stolze, Frieder Loch, Matthias Baldauf, Florian Alt, Christina Schneegass, Thomas Kosch, Teresa Hirzle, Shadan Sadeghian, Fiona Draxler, Kenan Bektas, Katrin Lohan, and Pascal Knierim (Eds.). ACM, New York, NY, USA, 359–363. doi:10.1145/3603555.3608573

[50] Michael Pirson and Deepak Malhotra. 2011. Foundations of Organizational Trust: What Matters to Different Stakeholders? *Organization Science* 22, 4 (2011), 1087–1104. doi:10.1287/orsc.1100.0581

[51] Sónia Rafael and Matilde Reis. 2024. Guidelines for Sustainable Online Behaviors. Green Computing Practices to Reduce the Digital Carbon Footprint. In *Advances in Design and Digital Communication IV*, Nuno Martins and Daniel Brandão (Eds.). Springer Series in Design and Innovation, Vol. 35. Springer Nature Switzerland, Cham, 261–275. doi:10.1007/978-3-031-47281-7{_}21

[52] Mihai Sanduleac, Dorel Stanescu, Carmen Stanescu, and Monica Florea. 2017. Energy awareness, an important goal for empowering the end customer. In *2017 International Conference on Optimization of Electrical and Electronic Equipment (OPTIM) & 2017 Intl Aegean Conference on Electrical Machines and Power Electronics (ACEMP)*. IEEE, 599–604. doi:10.1109/OPTIM.2017.7975034

[53] Nadine Schlicker, Kevin Baum, Alarith Uhde, Sarah Sterz, Martin Hirsch, and Markus Langer. 2023. A Micro and Macro Perspective on Trustworthiness: Theoretical Underpinnings of the Trustworthiness Assessment Model (TrAM). (07 2023). doi:10.31234/osf.io/qhwvx

[54] Sivan Schwartz, Avi Yaeli, and Segev Shlomov. 2023. Enhancing Trust in LLM-Based AI Automation Agents: New Considerations and Future Challenges. arXiv:2308.05391 [cs.AI] https://arxiv.org/abs/2308.05391

[55] Leif Sundberg and Jonny Holmström. 2023. Democratizing artificial intelligence: How no-code AI can leverage machine learning operations. *Business Horizons* 66, 6 (2023), 777–788. doi:10.1016/j.bushor.2023.04.003

[56] W. Syed, A. Bashatah, K. Alharbi, S. S. Bakarman, S. Asiri, and N. Alqahtani. 2024. Awareness and Perceptions of ChatGPT Among Academics and Research Professionals in Riyadh, Saudi Arabia: Implications for Responsible AI Use. *Medical Science Monitor* 30 (Jul 2024), e944993. doi:10.12659/MSM.944993

[57] Chandan Kumar Tiwari, Mohd. Abass Bhat, Shagufta Tariq Khan, Rajaswaminathan Subramaniam, and Mohammad Atif Irshad Khan. 2024. What drives students toward ChatGPT? An investigation of the factors influencing adoption and usage of ChatGPT. *Interactive Technology and Smart Education* 21, 3 (2024), 333–355. doi:10.1108/ITSE-04-2023-0061

[58] Michelle ME Van Pinxteren, Ruud WH Wetzels, Jessica Rüger, Mark Pluymaekers, and Martin Wetzels. 2019. Trust in humanoid robots: implications for services marketing. *Journal of Services Marketing* 33, 4 (2019), 507–518.

[59] Jörg von Garrel and Jana Mayer. 2023. Artificial Intelligence in studies—use of ChatGPT and AI-based tools among students in Germany. *Humanities and Social Sciences Communications* 10, 1 (09 Nov 2023), 799. doi:10.1057/s41599-023-02304-7

[60] Alan R Wagner, Jason Borenstein, and Ayanna Howard. 2018. Overtrust in the robotic age. *Commun. ACM* 61, 9 (2018), 22–24.

[61] C. Wang, D. Sui, B. Zhang, X. Liu, J. Kang, Z. Qiao, and Z. Tu. 2024. A Framework for Effective Invocation Methods of Various LLM Services. arXiv:2402.03408 [cs.CL] https://arxiv.org/abs/2402.03408

[62] I. Weber, H. Linka, D. Mertens, T. Muryshkin, H. Opgenoorth, and S. Langer. 2024. *FhGenie: A Custom, Confidentiality-preserving Chat AI for Corporate and Scientific Use.* http://arxiv.org/pdf/2403.00039v1

[63] Magdalena Wischnewski, Nicole Krämer, Philipp Doebler, and Marie Beisemann. 2023. Development of a new Trust in AI scale. https://osf.io/j7wk8

[64] Ziwei Xu, Sanjay Jain, and Mohan Kankanhalli. 2024. Hallucination is Inevitable: An Innate Limitation of Large Language Models. arXiv:2401.11817 [cs.CL] https://arxiv.org/abs/2401.11817

[65] X. Zhang, X. Zhang, and H. Liu. 2024. Reflections on Enhancing Higher Education Classroom Effectiveness Through the Introduction of Large Language Models. *Journal of Modern Education Research* 3 (2024), 19. doi:10.53964/jmer.2024019

[66] Mingji Zhou, Wei Chen, Senliang Zhu, Tianyang Cai, Ji Yu, and Guoyu Dai. 2023. Application of large language models in professional fields . In *2023 11th International Conference on Information Systems and Computing Technology (ISCTech)*. IEEE Computer Society, Los Alamitos, CA, USA, 142–146. doi:10.1109/ISCTech60480.2023.00033

[67] Justyna Łapińska, Iwona Escher, Joanna Górka, Agata Sudolska, and Paweł Brzustewicz. 2021. Employees' Trust in Artificial Intelligence in Companies: The Case of Energy and Chemical Industries in Poland. *Energies* 14, 7 (2021). doi:10.3390/en14071942