IACIS
Proceedings of the 65th International Association for Computer Information Systems Conference - October 1 - 4, 2025 | Clearwater

A NEW WAY TO TEACH PROGRAMMING USING GENERATIVE AI AND MODULAR MASTERY THRESHOLD PEDAGOGY (MMTP)

Bryan Marshall, Georgia College & State University, bryan.marshall@gcsu.edu
Jaclyn Queen, Georgia College & State University, jaclyn.queen@gcsu.edu
Alison Shepherd, Georgia College & State University, alison.shepherd@gcsu.edu
Brad Fowler, Georgia College & State University, brad.fowler@gcsu.edu
Peter W. Cardon, University of Southern California, cardon@marshall.usc.edu

Keywords: competency-based education, modular learning, mastery-based assessment, higher education, authentic assessment

This paper presents the Modular Mastery Threshold Pedagogy (MMTP), a novel educational framework that synergistically combines three established approaches: mastery-based learning with its focus on complete skill acquisition, competency-based education that emphasizes demonstrable abilities, and modular learning that structures content into sequential building blocks. By organizing curriculum into competency-based modules with clear mastery thresholds, this approach emphasizes skill acquisition over point accumulation while maintaining traditional letter grades.

The system employs pass/fail rubrics with 100% mastery requirements, authentic assessment tasks, and opportunities for resubmission, fostering a growth mindset. Students progress through tiered modules (basic to mastery level) that correspond to traditional letter grades, providing both flexibility and academic rigor. In this paper, we detail our implementation of this framework in an introductory Python programming course featuring seven progressive modules that transform students from complete beginners to developers capable of building full-stack web applications with generative AI integration. Our implementation experiences reveal significant benefits including enhanced student motivation through clear progression pathways, improved assessment transparency, and deeper learning outcomes. The paper addresses implementation challenges including student resistance, instructor workload, and rubric alignment, while providing practical mitigation strategies for each. This approach not only meets contemporary educational demands for skills-focused instruction but also maintains institutional compatibility by integrating with existing academic frameworks, offering educators a pragmatic pathway to emphasize competency development in higher education.

BIG DATA APPLICATIONS IN LAW ENFORCEMENT: ALL THINGS CONSIDERED

Donald "Breck" Terheide, Ball State University, dbterheide@bsu.edu
Allen D. Truell, Ball State University, atruell@bsu.edu
Eric S. Green, Ball State University, esgreen2@bsu.edu

ABSTRACT

There is little doubt that big data applications have permeated nearly every aspect of law enforcement. Thus, law enforcement professionals seek to maximize the strengths and minimize the weaknesses of big data applications. Therefore, the purposes of this presentation are multifold: (1) to provide an overview of big data applications in law enforcement, (2) to examine the strengths of big data applications in law enforcement, and (3) to explore reported weaknesses of big data applications in law enforcement. The presentation will highlight insights from a law enforcement professional with decades of experience working with multiple local, state, and federal agencies.

Keywords: big data, law enforcement

INFORMATION SYSTEMS FACULTY USE OF LEARNING MANAGEMENT SYSTEM TOOLS: PROMOTING LEARNER ENGAGEMENT

Allen D. Truell, Ball State University, atruell@bsu.edu
Eric S. Green, Ball State University, esgreen2@bsu.edu
Edward J. Lazaros, Ball State University, ejlazaros@bsu.edu
Christopher B. Davison, Ball State University, cbdavison@bsu.edu

ABSTRACT

Information systems faculty know that promoting learner engagement is critical to long-term persistence. Learner engagement improves academic performance, communication, professional readiness, institutional retention rates, and student mental health. Therefore, the purposes of this presentation are multifold: (1) to provide an overview of selected learning management system tools and (2) to provide examples of how information systems faculty have used these learning management system tools to promote learner engagement. The presentation will highlight insights from information systems faculty's use of learning management system tools to promote learner engagement.

Keywords: information systems, learning management system, learner engagement

DETERMINANTS OF LLM USE: AN EXPLORATORY STUDY

Judy Wynekoop, Florida Gulf Coast University, jwynekoo@fgcu.edu

INTRODUCTION

Generative AI, or large language models (LLMs), such as ChatGPT, are in the early stage of use for systems development tasks such as identifying requirements. The growing use of LLMs in systems development is expected to impact the way software is developed (Cámara et al, 2023). The results of this pilot study of factors influencing students' perceptions and use of LLMs in software development, grounded in the User Acceptance of Information Technology (UTAUT) framework (Venkatesh, 2003), provide educators insight into how to introduce and train developers for the successful use of LLMs. The pilot was undertaken to inform the creation of an instrument to study factors impacting the adoption and use of LLMs in software development.

THE STUDY

The study builds on self-efficacy theory and the UTAUT model to explore student attitudes toward generative AI, their intention to use the tools, and their performance outcomes. Since technology has greatly changed since self-efficacy measures were developed, existing instruments may no longer be valid, and measures should be created for new technologies (Gupta & Bostrom, 2019; Marakas, et al., 2007). While the UTAUT framework has been extensively modified and validated across various contexts (Dwivedi et al., 2019; Kundu et al., 2021) and has evolved (Venkatesh et al, 2016), its application to LLM adoption requires reexamination of underlying constructs. Since UTAUT subsumed computer self-efficacy into the effort expectancy construct, this study reexamines these relationships specifically for LLM contexts. The investigation also explores the relationship between critical thinking and self-efficacy.

Undergraduate students enrolled in a systems analysis and design course used ChatGPT to identify user needs and requirements for application prototypes. The pedagogical intervention included a 20-minute training session on effective prompt construction, incorporating examples of successful prompts and their corresponding outputs to scaffold student learning. Data collection employed pre- and post-intervention surveys measuring personal characteristics, LLM perceptions, and usage intentions, using Likert-scale items adapted from established instruments (Halpern, 1998; Venkatesh et al., 2003; Wright et al, 2023). Outcome variables were the student's intent to use an LLM and score on an assignment analyzing the LLM output. If UTAUT assumptions are confirmed, measures of LLM self-efficacy, performance expectancy and effort expectancy should be positively related to intent to use the LLM.

IMPLICATIONS AND CONCLUSIONS

This study tests measures of LLM self-efficacy and performance and effort expectancy, supporting assertions that such measures must be domain specific, as well as investigating whether LLM self-efficacy is captured by LLM effort expectancy, as indicated by the original UTAUT model (Venkatesh et al., 2003). The relationship of critical thinking and self-efficacy is unclear (Stajkovic, et al., 2018) – this study will test the relationship of critical thinking to LLM self-

efficacy, potentially providing guidance as to whether teaching students critical thinking skills will improve LLM self-efficacy and thereby improve LLM usage.

Preliminary results confirm predicted relationships. Improved self-efficacy and performance and effort expectancy after the treatment support the idea that individuals who are unsure of their ability to use an LLM to assist requirements identification can improve their skills and perceptions after brief training and use and the positive relationship between LLM self-efficacy and the outcome variables demonstrates the impact of self-efficacy on successful LLM use.

REFERENCES

Cámara, J., Troya, J., Burgueño, L. & Vallecillo, A. (2023). On the assessment of generative AI in modeling tasks: an experience report with ChatGPT and UML. *Software and Systems Modeling*, *22*(3), 781-793.

Dwivedi, Y.K., Rana, N.P., Jeyaraj, A., Clement, M. & Williams, M.D. (2019). Re-examining the Unified Theory of Acceptance and Use of Technology (UTAUT): Towards a revised theoretical model. *Information Systems Frontiers, 21*, 719–734.

Gupta, S., & Bostrom, R. P. (2019). A revision of computer self-efficacy conceptualizations in information systems. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, *50*(2), 71-93.

Halpern, D. (1998). Teaching critical thinking for transfer across domains. *American Psychologist*, 53(4), 449-455.

Kundu, A., Bej, T., & Dey, K. N. (2021). Investigating effects of self-efficacy and infrastructure on teachers' ICT use, an extension of UTAUT. *International Journal of Web-Based Learning and Teaching Technologies, 16*(6), 1-21.

Marakas, G.M., Johnson, R.D. , Clay, P. (2007). The evolving nature of the computer self-efficacy construct: An empirical investigation of measurement construction, validity, reliability and stability over time. *Journal of the Association for Information Systems*, *8*(1), 16-46.

Stajkovic, A.D., Bandura, A., Locke, E.A., Lee, D. & Sargent, K. (2018). Test of three conceptual models of influence of the big five personality traits and self-efficacy on academic performance: A meta-analytic path-analysis. *Personality and Individual Differences, 120,* 238-245.

Venkatesh, V., Morris, M.G., Davis, G.B. & Davis, F.D. (2003). User acceptance of information technology: toward a unified view. *MIS Quarterly*, *27*, (3), 425-478.

Venkatesh, V., Thong, J.Y.L, Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association of Information Systems*, *17*(S328-376).

Wright, K., Antonucci, Y.L., Anderson, L. & Townsend, A. (2023). Engaging students with "low-code" model driven development: Self-efficacy beliefs in an introductory MIS course. *Proceedings of the 56th Hawaii International Conference on Systems Sciences*, Maui, Hawaii, United States.

CONFIRMING OR EXPLORING WITH AI? THE IMPACT OF INTUITION AND ANALYSIS IN DECISION-MAKING STYLES

Fatih Çetin, Baskent University, fcetin@baskent.edu.tr
Markus Launer, Ostfalia University of Applied Sciences, m-a.launer@ostfalia.de
Joanna Paliszkiewicz, Warsaw University of Life Sciences, joanna_paliszkiewicz@sggw.edu.pl

ABSTRACT

While artificial intelligence (AI) becomes increasingly integrated into decision-making environments, understanding how individuals incorporate AI into their cognitive processes is crucial. This study examines how people with varying decision-making styles—defined by levels of analytical reasoning and intuition—engage with AI, specifically whether they use it to validate decisions already made or to generate new ideas before deciding. Drawing on dual-process models of cognition (Dane & Pratt, 2007), the research classifies users by their preference and capability for intuitive and analytical thinking.

The study involved 1,360 participants from different countries. Firstly, a cluster analysis was conducted to categorize individuals into distinct decision-making profiles. Two primary groups emerged: Rational Thinkers—comprising Analytic, Planning, and Knowing subtypes—and Intuitive Thinkers—including Unconscious Big Picture, Spontaneous Quick, Heuristics Expert, Slow Unconscious, Emotions, and Anticipation subtypes. Each group was further divided into high and low levels, resulting in combined profiles representing diverse decision-making styles. Then, participants' use of AI was examined through two main lenses: confirmation—where a decision is made independently and then verified using AI, and exploration—where AI is first used to propose insights or alternatives, which are then processed through analysis or intuition. The results indicate that individuals who score high in both analytical and intuitive domains—referred to as *wise decision-makers*—are significantly more inclined to use AI for confirmation than those with low intuitive tendencies, regardless of their level of analytical skill. This pattern suggests that balanced cognitive profiles prioritize personal judgment but value AI as a tool for reinforcement and error-checking (Logg, Minson, & Moore, 2019). Moreover, wise decision-makers also demonstrate greater use of AI for exploratory purposes than those categorized as *analyzers*—individuals with high analytical capacity but low intuition. While analyzers rely heavily on structured, logical reasoning, they may lack the cognitive openness to fully engage with AI-generated possibilities (Akinci & Sadler-Smith, 2012). Conversely, wise decision-makers appear more cognitively flexible, using AI to broaden their perspectives and refine judgments (Glikson & Woolley, 2020).

These findings underscore the importance of cognitive style in shaping how individuals interact with AI systems. Rather than viewing AI as a replacement for human decision-making, wise decision-makers leverage AI as a complement—either to confirm well-founded judgments or to expand the decision-making landscape through exploratory insight. This dual capacity reflects a more sophisticated integration of AI into cognitive processes (Shrestha, Ben-Menahem, & von Krogh, 2019).

Keywords: Intuition, Analysis, Artificial Intelligence, Decision making styles

REFERENCES

Akinci, C., & Sadler-Smith, E. (2012). Intuition in management research: A historical review. *International Journal of Management Reviews, 14*(1), 104–122. https://doi.org/10.1111/j.1468-2370.2011.00313.x

Dane, E., & Pratt, M. G. (2007). Exploring intuition and its role in managerial decision making. *Academy of Management Review, 32*(1), 33–54. https://doi.org/10.5465/amr.2007.23463682

Glikson, E., & Woolley, A. W. (2020). Human trust in artificial intelligence: Review of empirical research. *Academy of Management Annals, 14*(2), 627–660. https://doi.org/10.5465/annals.2018.0057

Logg, J. M., Minson, J. A., & Moore, D. A. (2019). Algorithm appreciation: People prefer algorithmic to human judgment. *Organizational Behavior and Human Decision Processes, 151*, 90–103. https://doi.org/10.1016/j.obhdp.2018.12.005

Shrestha, Y. R., Ben-Menahem, S. M., & von Krogh, G. (2019). Organizational decision-making structures in the age of artificial intelligence. *California Management Review, 61*(4), 66–83. https://doi.org/10.1177/0008125619862257

ADDRESSING IMPLICIT BIAS IN TEACHING AND ASSESSMENT: ETHICAL CHALLENGES AND EVIDENCE-BASED INTERVENTIONS

Schwartz, Jessica, Western Governors University, jess.schwartz@wgu.edu
Adams, April, Western Governors University, april.adams@wgu.edu
Lively, Charles, Western Governors University, charles.lively@wgu.edu

INTRODUCTION

Implicit bias in higher education continues to shape instructional methods, classroom dynamics, and student assessment in ways that can perpetuate inequity and hinder academic outcomes. This study examined the ethical implications of implicit bias in teaching and grading practices, with a focus on information systems and computing education. Drawing from interdisciplinary research in neuroscience, educational psychology, and institutional case studies, the analysis outlines how unconscious biases influence teacher expectations, disciplinary actions, grading outcomes, and faculty evaluations.

Specific attention is given to phenomena such as the Pygmalion effect, the Matilda effect in STEM, name-based grading disparities, and the influence of algorithmic bias in AI-powered assessment systems (Patel et al, 2021). Empirical examples, including blind grading trials, mentorship program reforms, and restorative justice initiatives, illustrate how targeted interventions can mitigate bias and improve equity (Okilwa, 2022). This study proposed a framework of ethical and practical strategies for educators and institutions committed to fostering inclusive and equitable learning environments. The goal is to contribute to the ongoing dialogue on academic fairness and inform future policy development in postsecondary education.

RACIAL DISPARITY IN DISCIPLINE

Implicit bias in higher education persists in shaping grading, instruction, and student outcomes in inequitable ways, particularly in computing and information systems disciplines. This study explored how unconscious bias affects academic environments, contributing to disparities in assessment, discipline, and mentorship. Through interdisciplinary analysis and empirical evidence, this work presents ethical concerns and introduces practical strategies to reduce bias, making the topic highly relevant for participants committed to inclusive pedagogy and ethical use of technology.

BASIS OF THE STUDY

This study synthesizes findings from peer-reviewed literature, institutional case studies, and psychological experiments. It draws on data regarding race- and gender-based disparities in grading, discipline, and faculty evaluations, along with research into algorithmic bias in AI grading tools (Gilliam et al., 2016; Okonofua & Eberhardt, 2015). Key sources include field experiments on name-based bias, studies on the Matilda and Pygmalion effects, and audits of automated assessment systems (Patel et al, 2021).

The data were analyzed to identify patterns of systemic bias and to evaluate the effectiveness of mitigation strategies such as blind grading, restorative justice practices, and equity-focused AI

design (Ladson-Billings, 2006). The analysis aims to demonstrate the widespread nature of implicit bias and the need for systemic interventions rooted in ethics, transparency, and distributive justice.

IMPLICATIONS OF THE STUDY

The implications of this study are both practical and ethical. It offers a framework for higher education institutions to promote equity by redesigning assessment systems, rethinking faculty development, and auditing educational technologies. Educators, technologists, and administrators are urged to implement reforms that address not just individual behavior but institutional structures that reproduce bias.

CONCLUSION

Confronting implicit bias requires more than raising awareness. It demands systemic change. This study concludes that integrating ethical principles into institutional practices through blind grading, AI oversight, equity audits, and educator training can help dismantle structural inequities in computing and IS education. Higher education institutions must move from reactive policies to proactive ethical design to ensure fair, inclusive academic environments.

REFERENCES

Gilliam, W. S., Maupin, A. N., Reyes, C. R., Accavitti, M., & Shic, F. (2016). Do early educators' implicit biases regarding sex and race relate to behavior expectations and recommendations of preschool expulsions and suspensions? *Yale University Child Study Center*.

Ladson-Billings, G. (2006). From the achievement gap to the education debt: Understanding achievement in U.S. schools. *Educational Researcher, 35*(7), 3–12.

Okilwa, N. (2022). A review of Oakland USD following an OCR investigation. *Global Education Review*.

Okonofua, J. A., & Eberhardt, J. L. (2015). Two strikes: Race and the disciplining of young students. *Psychological Science*, 26(5), 617–624.

Patel, S. R., St Pierre, F., Velazquez, A. I., Ananth, S., Durani, U., Anampa-Guzman, A., Castillo, K., Dhawan, N., Oxentenko, A.S., & Duma, N. (2021). The Matilda Effect: Underrecognition of Women in Hematology and Oncology Awards. *Oncologist, 26*(9): 779-786.

TOWARD SMARTER CYBERSECURITY: LEVERAGING AI FOR SOFTWARE UNDERSTANDING

Alan Stines, Middle Georgia State University, alan.stines@mga.edu

PROPOSED STUDY

This study examines the application of artificial intelligence (AI) in offensive cybersecurity, focusing on improving software understanding and detecting vulnerabilities in complex, interconnected systems. The research is relevant to IACIS conference participants because it aligns with current needs for scalable, automated solutions to cybersecurity threats (Moreno et al., 2025). As organizations increasingly rely on third-party and embedded software systems, the ability to analyze software without source code is becoming essential.

BASIS OF STUDY

This study is based on a structured review of recent literature, including peer-reviewed journal articles, technical conference proceedings, and government publications from organizations such as CISA, NSA, and DARPA (Cybersecurity and Infrastructure Security Agency et al., 2025; Ghormley et al., 2025; Software Understanding for National Security (SUNS), 2023). Sources were identified using search terms like 'AI fuzzing', 'autonomous penetration testing', and 'software understanding'. Materials were categorized by research themes and evaluated for their contribution to vulnerability discovery, software transparency, and legal considerations (Harguess & Ward, 2025).

The literature highlights several active research areas where AI enhances traditional techniques such as fuzzing and symbolic execution. It also reveals operational and legal gaps, including limitations on using commercial AI platforms for security testing and a lack of scalable tools for system-of-systems analysis. The review informed the design of a conceptual IoT cybersecurity lab, which will evaluate practical applications of these tools in controlled environments (Bhandari et al., 2024).

IMPLICATIONS OF THE STUDY

The study implies that further work is needed to integrate AI tools into cybersecurity operations. Cross-disciplinary efforts between AI, cybersecurity, and policy are necessary to resolve barriers to adoption. Public-private partnerships, academic testing environments, and clearer governance frameworks will ensure that AI-enabled techniques are lawful and practical (Valencia, 2024).

CONCLUSIONS

AI presents promising capabilities for proactive cybersecurity testing and software analysis. While current tools remain limited in scope and generalizability, structured environments like the proposed IoT lab can provide the needed foundation for evaluating, improving, and safely deploying these technologies. This research contributes to a growing work that bridges technical advancement with ethical and institutional responsibility.

REFERENCES

Bhandari, G. P., Assres, G., Gavric, N., Shalaginov, A., & Grønli, T.-M. (2024). IoTvulCode: AI-enabled vulnerability detection in software products designed for IoT applications. *International Journal of Information Security*, *23*(4), 2677–2690. https://doi.org/10.1007/s10207-024-00848-6

Cybersecurity and Infrastructure Security Agency, Defense Advanced Research Projects Agency, Office of the Under Secretary of Defense for Research and Engineering, & National Security Agency. (2025). *Closing the Software Understanding Gap*. https://www.cisa.gov/sites/default/files/2025-01/joint-guidance-closing-the-software-understanding-gap-508c.pdf

Ghormley, D., Amon, T., Harrison, C., & Loffredo, T. (2025). *The National Need for Software Understanding: The Present Crisis, Technical Capability Gaps, and Path Forward*. https://www.sandia.gov/app/uploads/sites/224/2025/03/The-National-Need-for-Software-Understanding-v1.0.pdf

Harguess, J., & Ward, C. M. (2025). *Offensive Security for AI Systems: Concepts, Practices, and Applications*. http://arxiv.org/abs/2505.06380

Moreno, A. C., Hernandez-Suarez, A., Sanchez-Perez, G., Toscano-Medina, L. K., Perez-Meana, H., Portillo-Portillo, J., Olivares-Mercado, J., & García Villalba, L. J. (2025). Analysis of Autonomous Penetration Testing Through Reinforcement Learning and Recommender Systems. *Sensors*, *25*(1), 211. https://doi.org/10.3390/s25010211

Software Understanding for National Security (SUNS). (2023). *Synopsis of the March 2023 Software Understanding for National Security (SUNS) Workshop*. https://www.sandia.gov/app/uploads/sites/224/2024/04/SUNS-2023-Workshop-Synopsis-SAND2024-04945R.pdf

Valencia, L. J. (2024). *Artificial Intelligence as the New Hacker: Developing Agents for Offensive Security*. http://arxiv.org/abs/2406.07561

AI'S IMPACT ON CENTRALIZATION AND DECENTRALIZATION OF DECISION-MAKING IN FIRMS

Tzuyi Chan, University of Southern California, tzuyicha@usc.edu
Peter Cardon, University of Southern California, cardon@marshall.usc.edu

The integration of artificial intelligence (AI) into business operations is rapidly transforming how firms make decisions, restructure their organizations, and manage strategy. More importantly, it is redefining managerial roles. In today's rapidly globalized and highly competitive environment, AI-driven decision-making has become indispensable (Schmitt, 2023). What was once regarded as a supplementary tool is now a key force in shaping competitive advantage.

At the same time, AI technologies have evolved to become more accurate and diverse, with various types offering distinct business benefits, from supporting sound decision-making to boosting employee productivity and enhancing operational efficiency (Lumenalta, 2025). For instance, specialized AI (or Narrow AI) is widely used to perform routine tasks and make predictions within specific domains. Generative AI, on the other hand, can be applied across a broader range of functions, exhibiting human-like reasoning, learning, and problem-solving capabilities (Lumenalta, 2025). However, both Narrow AI and Generative AI lack true autonomy – they cannot independently initiate actions or make decisions without human input (Coshow, Gao, 2024). More recently, Agentic AI has emerged as a powerful new frontier. This type of AI system not only handles fundamental data analysis and routine tasks but can also make decisions and drive performance (Coshow, Gao, 2024). Notably, firms can authorize Agentic AI systems to operate independently, granting them the ability to act, drawing from memory, developing plans, and taking steps toward achieving business goals (*Salesforce*).

As AI tools become more sophisticated and firms increasingly adopt them to enhance data-driven decisions, automate workflows, predict consumer behavior, and optimize resource allocation (Mahabub, 2025), AI has significantly affected both strategic and operational activities. While AI adoption in firms can bring many benefits—such as increased productivity, enhanced firm performance, and improved ability to predict market trends to make more sound decisions—relatively little attention is paid to its organizational consequences. More specifically, as organizations increasingly rely on AI-generated recommendations, several key questions arise: Is AI shifting firms toward more centralized decision-making, where top executives have stronger control over data and insights? Or is it becoming more decentralized by empowering employees across departments and at various levels with real-time information and greater decision-making autonomy? Moreover, traditional managerial authority might be doubted, challenging the traditional managerial decision-making process, especially when AI systems outperform human judgment in both speed and accuracy.

While most of the literature on AI adoption in businesses is related to how AI-driven decision-making affects firm performance, relatively few studies focus on how organizational structures and managerial roles change after AI adoption. This study explores how AI reshapes firm structure and strategic management, focusing on two interrelated dynamics. First, it examines whether AI

adoption leads firms to adopt more centralized or decentralized structures, or hybrid models that differentiate between strategic and operational decision-making. Second, it investigates how managerial roles evolve in an AI-enhanced environment, especially in terms of authority, trust, and decision legitimacy. As AI systems become increasingly influential and accurate, managers may find their decisions questioned by employees who view AI outputs as more reliable or impartial. These shifts will pose new challenges for leadership, communication, and organizational culture.

To address this issue, this study fills the gap by combining case studies, theoretical modeling, and practical interviews (to be conducted in July and August 2025 with 25 to 30 managers and executives in AI-mature firms) to access the timely and nuanced insights into how AI technology alters internal organizational dynamics. Ultimately, this research aims to offer a comprehensive understanding of how firms can adapt, learn, and navigate the ongoing transformation brought about by AI, and it also proposes recommendations and future implications for firms.

ASSESSMENT OF LEARNING IN IS: A FRAMEWORK FOR GENAI AND LEARNER PROGRESSION

Joseph M. Woodside, Stetson University, joseph.m.woodside@gmail.com
Fred K. Augustine, Jr., Stetson University, fagusti@stetson.edu
William Sause, Stetson University, wsause@stetson.edu

OVERVIEW AND IMPORTANCE: CHANGING THE WORLD OF WORK AND ASSESSMENT IN IS

Generative AI (GenAI) is transforming education, industry, and society's landscapes, and educators must not only embrace the evolving technology but also prepare future leaders to navigate and leverage it. Sherif Kamel, Dean of the School of Business at The American University in Cairo, emphasizes the importance of integrating GenAI into teaching, research, and program delivery in a human-centered, purpose-driven way (AACSB, 2024a; Rafalski, 2025). GenAI can be viewed as another method to enhance innovation and support the mission of schools. When integrated with other technological advancements, GenAI allows for new and innovative educational approaches, including interactive and experiential learning, and creates personalized assessment and learning pathways. In addition, GenAI provides several benefits for students, including learning tailored to individual needs, improved cross-disciplinary integration for a more holistic educational experience, and enhanced creativity through tools that stimulate innovation and problem-solving. It also promotes the democratization of education and inclusiveness by making high-quality, personalized learning accessible to a broader audience (Fui-Hoon Nah, Zheng, Cai, Siau, & Chen, 2023; AACSB, 2024a; AASCB, 2024b).

According to a Deloitte survey, while 62 percent of business and technology leaders are excited about GenAI, only 22 percent felt highly prepared to address talent challenges associated with its adoption (AACSB, 2024a). The lack of technical talent and skills is a substantial barrier to GenAI's broader use, leading organizations to adapt their talent strategies and employee skillsets. Industry organizations are prioritizing AI literacy across all positions, including understanding how to use GenAI effectively. Adaptability is becoming essential as organizations adjust to the rapid changes driven by GenAI. According to an AACSB survey, the changing demands of the workforce are also driving shifts in faculty expectations, with 71% of faculty reporting significant changes in their roles due to digital transformation. As GenAI influences both teaching and research practices, faculty engagement and support are critical for successfully incorporating the technology into educational frameworks and shaping the leaders of tomorrow (Saetra, 2023; AACSB, 2024a; AACSB, 2024b).

BASIS OF THE STUDY AND DATA SOURCE

This paper seeks to identify the best practices and policy implications for the use of GenAI within the assessment of learning in information systems. Assessment data will be collected from a core information systems course completed by all undergraduate students. A primary curricular change consisting of GenAI instruction and course integration will be included beginning in August 2025. Assessment data will be compared to previous assurance of learning benchmarks. The data analysis will be reviewed to measure student results using a combination of both GenAI and non-

GenAI techniques and best practices for building learning scaffolding throughout the curriculum, improving student learning outcomes, and ensuring post-graduation career success.

IMPLICATIONS AND CONCLUSIONS

This paper will present findings as identified through quantitative and qualitative methods, which extend and enhance prior literature and understanding of AI for assessment of learning in IS. Prior studies focus on the IS curriculum, general assessment, or the use of AI in education. This study will review the best practices for assessment measures for student learning outcomes using GenAI within the information systems discipline and foundational curriculum. While current curriculum design guidelines focus on lower levels of learning, the goal is to identify methods of AI to move students up Bloom's Taxonomy and increase Learner Progression. Bloom's taxonomy offers a useful scale for assessing student competencies (Bloom, 1968; IAforTeachers, 2023). In a professional setting, competency refers to the successful completion of tasks as part of routine job requirements. In the IS2020 framework, a cautious approach is taken with a focus on entry-level competencies of graduates, primarily measured through assignment completion as part of studies. Identifying the gaps between professional competencies, curricular competencies, and tasks is a critical review area (Leidig & Salmela, 2020).

Educators play a crucial role in developing well-rounded talent by equipping students with essential skills such as AI literacy, complex thinking skills, and integrative abilities. Fostering an ethical mindset and a commitment to lifelong learning through practical, cross-disciplinary, and purpose-driven experiences is key to student success (AACSB, 2024a; AASCB, 2024b). GenAI can play an essential role in improving student learning and supporting accreditation efforts. Furthermore, by providing greater insights into individual student performance, AI can help ensure that the curriculum content aligns with accreditation standards. AI can automate data analysis to identify patterns in student work, generate reports to aid data-driven decision-making, and help maintain academic rigor and integrity. Additionally, AI can assist in developing course materials, such as questions and rubrics, while providing personalized, immediate feedback to students. Ultimately, the use of GenAI can enhance course design, leading to more effective teaching and improved student learning outcomes (Bisoux, 2024).

REFERENCES

AACSB. (2024a). Building Future-Ready Business Schools with Generative AI. Retrieved January 22, 2025, from https://www.aacsb.edu/insights/reports/building-future-ready-business-schools-with-generative-ai.

AACSB. (2024b). AACSB Report Offers Business School Guidance on GenAI. Retrieved March 2, 2025, https://www.aacsb.edu/media-center/news/2024/04/aacsb-report-offers-business-school-guidance-on-genai.

Bisoux, T. (2024). How Can AI Support Your Accreditation Efforts? AACSB. Retrieved March 20, 2025, from https://www.aacsb.edu/insights/articles/2024/09/how-can-ai-support-your-accreditation-efforts.

Bloom, B.S. (1968). Learning for Mastery. In Evaluation Comment. UCLA Center for the Study of Evaluation and Instructional Programs.

Fui-Hoon Nah, F., Zheng, R., Cai, J., Siau, K., & Chen, L. (2023). Generative AI and ChatGPT: Applications, challenges, and AI-human collaboration. *Journal of Information Technology Case and Application Research*, 25(3), 277–304.

IAforTeachers. (2023). Medium. Retrieved on January 24, 2025, from https://fsanta.medium.com/theoretical-background-on-artificial-intelligence-and-education-99e7c383deb2.

Leidig, P., Salmela, H. (2020). IS2020 A Competency Model for Undergraduate Programs in Information Systems. *The Joint ACM/AIS IS2020 Task Force*. Retrieved April 25, 2025, from: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/is2020.pdf.

Rafalski, K. (2025). AI Impact on Education: Its Effect on Teaching and Student Success. Retrieved May 16, 2025, from https://www.netguru.com/blog/ai-in-education.

Saetra, H.S. (2023). Generative AI: Here to stay, but for good? *Technology in Society*, Volume 75, 102372, ISSN 0160- 791X.

IMPLEMENTING AN ORGANIZATIONAL AI APPLIANCE DEPLOYER (OAAD) FOR AI ADOPTION STANDARDIZATION AND IMPACT STUDIES THROUGH ADOPTION EXPERIMENTATION

Pius A. Onobhayedo, University of Southern California, po_988@usc.edu
Peter Cardon, University of Southern California, cardon@marshall.usc.edu

The transformative potential of artificial intelligence (AI) necessitates standardized frameworks to guide organizations toward effective and ethical adoption. We examine the path to organizational AI adoption standardization, structured around the five-pillar framework—Strategy, Data, Technology, People, and Governance—as proposed in Arm's AI Readiness Index: Measuring Organizational Preparedness for Artificial Intelligence (2024). Drawing on recent research, we assess current progress, identify barriers, and outline pathways for advancing AI standardization.

Extant research reveals an adoption-strategy paradox which in our opinion requires further research attention. While over 80% of organizational global leaders believe that it is urgent for their organizations to embrace AI and a significant number aligning their budget to match their belief, less than 40% have measurable KPIs, underscoring the need for robust roadmaps (Arm, 2024; Amrollahi & Ghapanchi, 2023). Besides strategy poverty, data readiness is hindered by silos and quality issues, with 60% of organizations facing challenges, necessitating standardized data protocols (Arm, 2024; Hradecky et al., 2024). Technology adoption progress further reveals edge AI optimization lags, highlighting the need for scalable and secure infrastructure (Arm, 2024; Wirtz et al., 2022). The People pillar faces a critical skills gap, with only 30% of organizations offering comprehensive AI training, calling for standardized workforce development (Arm, 2024; Selten & Klievink, 2024; World Economic Forum, 2024). Governance remains underdeveloped, with only 35% addressing ethical concerns like bias, aligning with global calls for standardized frameworks such as the EU AI Act (Arm, 2024; Taeihagh et al., 2021; Zuiderwijk et al., 2021). The global AI Readiness Index further indicates regional and industry disparities (Arm, 2024) which could be even more pronounced if the referenced Arm (2024) study is extended to Africa.

By integrating insights from Arm (2024), Grisenthwaite (2025), and other studies (e.g., Hutter & Jung, 2024; Manyika et al., 2017), we propose a new approach that harmonizes adoption fostering with research, rather than only habitually taking the approach to asking organizations about what they are doing or hope to do, through surveys. We refer to our approach as adoption experimentation. As a step towards adoption experimentation and knowing the complexity of AI infrastructure and the requisite competencies, we have designed a way to quickly implement an AI appliance within organizations, informed by expert researchers, customizable for each organization's data pipeline and business goals, and adjustable as AI infrastructure progresses. In this conference, we present OAAD (Organizational AI Appliance Deployer) designed and developed for this purpose. We believe that this approach will not only foster adoption with more strategic intent and expert handholding, but it will also give the researchers the opportunity to progressively study the impact and dynamics of AI adoption in the organization. OAAD is designed to essentially provide a quick way to automate the pipelining of requisite organizational data, flexibly deploy customized AI agents aligned with the organizational goals, along with tools

for monitoring the health of the appliance subsystems, taking an edge first policy to better guarantee data privacy.

REFERENCES

Amrollahi, A., & Ghapanchi, A. H. (2023). Artificial intelligence adoption in professional service firms: A multiple case study. Information & Management, 60(5), 103789. https://doi.org/10.1016/j.im.2023.103789

Arm. (2024). *AI readiness index: Measuring organizational preparedness for artificial intelligence*. https://armkeil.blob.core.windows.net/developer/Files/pdf/report/arm-ai-readiness-index-full-report.pdf

Chui, M., Manyika, J., Miremadi, M., Henke, N., Chung, R., Nel, P., & Malhotra, S. (2018). *Notes from the AI frontier: Insights from hundreds of use cases*. McKinsey Global Institute. https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-insights-from-hundreds-of-use-cases

Grisenthwaite, R. (2025, April 25). Tackling AI's challenges starts with strong architectural foundations. *Computing*. https://www.computing.co.uk/opinion/2025/tackling-ai-s-challenges-strong-architectural-foundations

Hradecky, D., Kromer, L., & Kenney, M. (2024). Determinants of artificial intelligence adoption: Research themes and future directions. *Information Technology and Management, 25*(3), 245–262. https://doi.org/10.1007/s10799-024-00412-5

Hutter, K., & Jung, T. (2024). Organizational readiness to adopt artificial intelligence in the exhibition sector in Western Europe. *International Journal of Information Management, 74*, 102645. https://doi.org/10.1016/j.ijinfomgt.2023.102645

Manyika, J., Chui, M., Miremadi, M., Bughin, J., George, K., Willmott, P., & Dewhurst, M. (2017). *A future that works: Automation, employment, and productivity*. McKinsey Global Institute. https://www.mckinsey.com/featured-insights/digital-disruption/harnessing-automation-for-a-future-that-works

McKinsey Global Institute. (2025). *The state of AI: How organizations are rewiring to capture value*. McKinsey & Company. https://www.mckinsey.com/business-functions/quantumblack/our-insights/the-state-of-ai-how-organizations-are-rewiring-to-capture-value

Selten, F., & Klievink, B. (2024). Organizing public sector AI adoption: Navigating between separation and integration. *Government Information Quarterly, 41*(1), 101892. https://doi.org/10.1016/j.giq.2023.101892

Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2022). Exploring artificial intelligence adoption in public organizations: A comparative case study. *Public Management Review, 24*(3), 401–424. https://doi.org/10.1080/14719037.2020.1832075

World Economic Forum. (2024). *AI governance trends: How regulation, collaboration, and skills demand are shaping the industry*. https://www.weforum.org/publications/ai-governance-trends-how-regulation-collaboration-and-skills-demand-are-shaping-the-industry/

AUTHORIZED AUTHORSHIP OF AI

David B. Scibelli, Winthrop University, scibellid@winthrop.edu
Michael P. Whitney, Winthrop University, whitneym@winthrop.edu
Raquel Laverne Rhoades, Winthrop University, rhoadesr2@mailbox.winthrop.edu

ABSTRACT

This proposed research will focus on the role of the authorship of creative works through using Artificial Intelligence (AI) systems. From a scholarly lens perspective, the are standards and expectations to be used scholarly work at all levels in our field. As we bridge the innovative advancement of AI generated forms of data, information, and product deliverables, there is a gap in the traceability, ownership, and linkage to sourced sound body-of-knowledge. Stemming from this problem, how do we substantiate AI generated data in our works? In addition, is there a significance of identifying scholarly ownership when using generated data from Artificial Intelligence?

This meta-analysis will survey scholarly literature and the practices of the current Modern Era landscape. Further investigation will also examine legal cases and rulings to develop the degree of acceptance for which the populous has adopted the use of AI output.

Specific to this proposed research, leaning through the convergence of "quasi-open" data sources, the use of tertiary works and creative authorship is believed the basis of many newly founded works in many areas. In addition, the adoption of responsive AI use is at precipice of proliferation for many technology consumers, where AI systems are providing unsourced responses in authorized messaging. A simple example is the use of common web search services for which an AI generative answer is provided, not without the linkage the data sources. Expected as this technology hardens, the reliability of the AI authoritative answer will be with minimal error tolerance. Thereby, Artificial Intelligence will provide a reasonably correct answer to further implementation.

In conclusion, the notion of AI generative use of data in human works will plausibly be further substantiated over time, where the perception of use of data will be acceptable, given the construct that the laws and practices will continue to adopt and accept the innovation. As common observation, privacy laws for consumers were not strongly developed during the Internet growth, thereby allowing the technology to advance to great innovation bringing humans to this point in an interconnected landscape. Hypothetically, one may suggest hindering the traditional boundaries of the body-of-knowledge, which might progress the leap in the advancement of AI technology. As this proposed research comes to fruition, to what degree is the balance of innovation and traditional works to be kept in reaching the technology future?

ARTIFICIAL INTELLIGENCE IN EDUCATION AND RESEARCH: OPPORTUNITIES, CHALLENGES, AND ETHICAL CONSIDERATIONS

Joanna Paliszkiewicz, Warsaw University of Life Sciences, joanna_paliszkiewicz@sggw.edu.pl
Ireneusz Dąbrowski, Warsaw School of Economics, rekinpri@sgh.waw.pl

The aim of this study is to comprehensively explore how artificial intelligence (AI) influences the quality of education and scientific research. It investigates the evolving role of AI technologies—from automation to collaboration—and analyzes both the opportunities they present and the ethical challenges they pose. Given the increasing reliance on AI tools in academic environments, this research is highly relevant for IACIS participants, particularly those focused on the intersection of information systems, educational effectiveness, and institutional integrity.

This research is based on an extensive review of academic literature, institutional reports, and current AI applications in the educational and scientific domains. It evaluates both empirical findings and theoretical perspectives related to the development and deployment of AI systems such as adaptive learning platforms, language models, and research assistants. Key tools discussed include ChatGPT, ALEKS, Knewton, Elicit, and ResearchRabbit.

The analysis synthesizes how AI tools affect personalization, efficiency, and access to knowledge, while also highlighting risks such as ethical ambiguity, algorithmic bias, and the erosion of critical thinking. The review draws on multidisciplinary sources to frame AI not as a replacement for human educators or researchers but as a partner in cognitive and academic endeavors (Paliszkiewicz & Gołuchowski, 2024). Special attention is given to trust in AI (Lukyanenko et al., 2022; Riedl, 2022), transparency, and regulatory responses, including the EU AI Act (Brown et al., 2022; Lombardi, 2023) and UNESCO/OECD recommendations.

The study suggests that responsible use of AI can significantly enhance the quality, accessibility, and personalization of educational and research processes. However, without adequate ethical frameworks (Díaz-Rodríguez et al., 2023), digital competencies (Araujo et al., 2020), and institutional policies, AI may undermine core academic values such as autonomy, authorship, and reflective learning. This necessitates critical awareness and human-centered approaches in system design and usage.

AI has the potential to revolutionize education and science by augmenting human capabilities and democratizing access to information. However, the success of AI integration depends not on technological sophistication alone, but on the capacity of educators, researchers, and institutions to use it wisely, ethically, and transparently. The research emphasizes the need to align AI adoption with educational values and to cultivate a culture of responsibility, critical thinking, and digital literacy. Technology should serve learning—not replace the learner.

REFERENCES

Araujo, T., Helberger, N., Kruikemeier, S., & De Vreese, C. H. (2020). In AI, we trust? Perceptions about automated decision-making by artificial intelligence. *AI & Society*, *35*(3), 611–623.

Brown, R., Truby, J., & Ibrahim, I. A. (2022). Mending Lacunas in the EU's GDPR and Proposed Artificial Intelligence Regulation. *European Studies: The Review of European Law, Economics and Politics*, *9*(1), 61–90. https://doi.org/10.2478/eustu-2022-0003

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López de Prado, M., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, *99*. https://doi.org/10.1016/j.inffus.2023.101896

Lombardi, A. (2023). Data protection regulation and artificial intelligence regulation: relationships, similarities and differences between GDPR and AI Act | Disciplina della tutela dei dati personali e regolazione dell'intelligenza artificiale: rapporti, analogie e differenz. *European Journal of Privacy Law and Technologies*, *2023*(2), 240–252.

Lukyanenko, R., Maass, W., & Storey, V. C. (2022). Trust in artificial intelligence: From a Foundational Trust Framework to emerging research opportunities. *Electronic Markets*, *32*(4), 1993–2020. https://doi.org/10.1007/s12525-022-00605-4

Paliszkiewicz, J., & Gołuchowski, J. (2024). Trust in artificial intelligence – future directions in: J. Paliszkiewicz, J. Gołuchowski, *Trust and Artificial Intelligence: Development and Application of AI Technology*. Routledge, Taylor and Francis https://doi.org/https://doi.org/10.4324/9781032633749

Riedl, R. (2022). Is trust in artificial intelligence systems related to user personality? Review of empirical evidence and future research directions. *Electronic Markets*, *32*(4), 2021–2051. https://doi.org/10.1007/s12525-022-00594-4

FROM FEAR TO COMPETENCY: GUIDING UNIVERSITY STAFF THROUGH THE GENERATIVE AI REVOLUTION

Brian Gardner, Pennsylvania State University, bkg113@psu.edu
Jennifer L. Breese, Pennsylvania State University, jzb545@psu.edu

ABSTRACT

The recent advancements in artificial intelligence (AI) research have been fueled by the rapid adoption of generative AI tools such as ChatGPT, Microsoft Copilot, Google Gemini, Perplexity, and DALL•E 3. Generative AI tools have been adapted to a wide variety of use cases – science, engineering, healthcare, software development, etc. – and created limitless opportunities for its use in enhancing our daily lives. Many individuals are concerned about how generative AI will impact them, some who carry fears about how it might significantly transform or even eliminate their role in the future. Introducing generative AI concepts to novice users should include an unbiased explanation of what it can and cannot so that everyone can begin to assess how the technologies may impact them in the future. The responses to the initial survey distributed to our business operations staff at a branch campus of a major university revealed a personal assessment of their competency with generative AI tools and reflections on how AI could help them do better in the workplace. The initial results of that study will form the basis of our research to understand how to prepare the workforce for the continued integration of generative AI in the workplace and how users having limited experience with the technology today can prepare themselves for how their current roles and responsibilities may operate in an AI-assisted world.

BASIS OF THE STUDY

A pilot survey was distributed to business operations personnel across various operating units at a branch campus of a major university. The respondents identified their current level of competence with the AI tools they have used to assist them with work-related tasks or personal projects. An expanded survey will be distributed to a wider audience where additional feedback will be provided and demographics for population comparisons. The additional data will help shape our research on how to develop structured educational offerings that ease our staff into the changes AI will bring to their roles on our campuses. We have already experienced staff headcount reductions unrelated to the adoption of AI, leaving the remaining staff responsible for covering the entire spectrum of tasks in their domain. One of our study objectives is to identify where AI can complement our workforce to compensate for the headcount gap. A second objective is to help our staff develop individual learning plans to master the relevant AI skills required to adapt to an AI-assisted work environment.

IMPLICATIONS OF THE STUDY

The sources of information about generative AI are unlimited, which may overwhelm or possibly discourage staff who are curious about the technology but do not know how to get started with using it. Our university is already promoting AI initiatives through a web portal that showcases many facets of how the technology is being used across our system. We foresee an opportunity to

develop AI competency centers at each branch campus that will promote responsible use of the technology and establish processes and procedures around its adoption for our local staff.

CONCLUSIONS

The number of individuals responding to our initial survey was limited; however, strong indicators of how our staff is using generative AI tools are already starting to emerge. Fifty percent of the fourteen respondents indicated they use generative AI tools in some capacity on a regular basis, most say they use it daily. The top three use cases where respondents indicated generative AI tools are being used include content creation, data collection/analysis, and self-improvement to understand how it works. Our next milestone is to distribute our survey with more targeted questions to start developing profiles of its current use as well as explore new ways in which it can complement our staff's current responsibilities. We also hope to set realistic expectations with our staff about what AI can and cannot do relative to any perceptions they may already have about its capabilities. Our research team may also find opportunities to leverage generative AI tools to devise a tailored instructional approach to help our staff increase their competence in the use of the tools for their specific use cases.

REFERENCES

Adarkwah, M. A. (2024). *GenAI-Infused Adult Learning in the Digital Era: A Conceptual Framework for Higher Education. Adult Learning*, 0(0). https://doi.org/10.1177/10451595241271161

Kuipers, Martijn & Prasad, Ramjee. (2022). *Journey of Artificial Intelligence*. Wireless Personal Communications. 123. 10.1007/s11277-021-09288-0, https://dl.acm.org/doi/10.1007/s11277-021-09288-0

Lee, D., Arnold, M., Srivastava, A., Plastow, K., Strelan, P., Ploeckl, F., Lekkas, D., Palmer, E. (2024). *The impact of generative AI on higher education learning and teaching: A study of educators' perspectives*. Computers and Education: Artificial Intelligence, 6, 100221.

Microsoft Copilot (n.d.). https://www.it.psu.edu/services/office365/microsoft-copilot/, retrieved 4/4/2025.

LEVERAGING AI-DRIVEN PREDICTIVE CYBER ANALYTICS FOR PROACTIVE THREAT HUNTING IN ENTERPRISE SECURITY

Mary Kotch, Pennsylvania State University, mnb104@psu.edu
Jennifer L. Breese, Pennsylvania State University, jzb545@psu.edu

ABSTRACT

In the rapidly evolving cyber threat landscape, organizations must shift from reactive to proactive threat detection strategies. Cybersecurity teams face an overwhelming number of security alerts, making it difficult to identify true threats amidst the noise. This research explores how AI-driven predictive analytics, integrated with Microsoft Sentinel, Data Lakes, and Large Language Models (LLaMA 2 and GPT-4), can transform cyber threat hunting by leveraging machine learning, natural language processing, and data correlation techniques. This study presents an LLM-driven predictive cyber analytics framework that aggregates security telemetry to detect anomalous user behaviors, phishing campaigns, malware activity, lateral movement, and insider threats. By utilizing predictive modeling, machine learning anomaly detection, and AI-driven triage, this research aims to improve decision-making, automate security operations, and enhance cyber resilience in organizations. Limitations include the high cost of training the model with the desired amount of data.

Keywords: Cybersecurity, AI, Predictive Analytics, Large Language Models, Machine Learning, Predictive Modeling

INTRODUCTION AND FRAMEWORK FOR AI-POWERED PREDICTIVE CYBER ANALYTICS

Cyber threats are becoming more sophisticated, requiring enterprises to adopt an AI-driven approach to cybersecurity. The traditional signature-based threat detection methods are no longer sufficient against advanced persistent threats (APTs) and zero-day attacks. Organizations need to leverage predictive analytics, AI, and machine learning models to anticipate, detect, and mitigate threats before they cause significant harm. The goal of this research is to strengthen the cybersecurity posture of a company and propose adoption more broadly.

This research addresses the following questions:
RQ1: How can AI-driven predictive analytics enhance threat hunting capabilities?
RQ2: What are the most effective machine learning models for detecting cyber threats in enterprise environments?
RQ3: How can organizations integrate LLMs with security telemetry to improve real-time threat detection?

The proposed framework follows a data-driven AI strategy, leveraging the following components:

1. Data Lake Integration for Unified Threat Analysis: Security logs from multiple sources (e.g., Microsoft Defender, Proofpoint, Palo Alto, Zscaler, and Qualys) are ingested into a centralized

Data Lake using Microsoft Sentinel. This approach enables correlation of threat indicators across multiple security platforms, allowing analysts to see the full attack chain.

2. Predictive Threat Models for Early Detection: We implement machine learning algorithms to predict phishing attacks, malware intrusions, privilege escalation attempts, and insider threats. These models analyze historical attack patterns and correlate logs across different platforms to provide a risk score for each user and asset.

3. LLM-Powered Anomaly Detection: By fine-tuning LLaMA 2 on cybersecurity incident reports and security logs, we enable natural language processing (NLP)-based threat correlation. GPT-4 is used to automate alert triage, summarizing threat intelligence reports and generating incident response playbooks.

4. AI-Driven Incident Triage in Microsoft Sentinel: Using GPT-4-powered AI automation, we classify alerts based on severity and probability of compromise. This significantly reduces false positives and allows security analysts to focus on high-risk threats.

DISCUSSION OF FINDINGS AND LIMITATIONS

Implementing AI-driven predictive analytics in cybersecurity yields the following benefits: (1) Early Detection of Cyber Threats: AI models detect anomalous behavior before an attack is fully executed, (2) Reduction in False Positives: Machine learning-based alert prioritization helps analysts focus on critical incidents, (3) Automated Threat Hunting: AI models continuously learn from attack patterns and enhance security response, (4) Improved Incident Response Time: AI-generated playbooks enable rapid mitigation of security threats.

Training the model with 2 years of data was cost prohibitive. Data was scaled back to one-year, security logs were stripped down to supply only the necessary characters lowering data size and in-turn cost. The scope and size and timeline of the LLM Training was delayed but met expected overall project expectations.

REFERENCES

Chowdhury, R. H., Prince, N. U., Abdullah, S. M., & Mim, L. A. (2024). The role of predictive analytics in cybersecurity: Detecting and preventing threats. *World Journal of Advanced Research and Reviews*, *23*(2), 1615-1623. https://doi.org/10.30574/wjarr.2024.23.2.2494

Danish, M. (2024). Enhancing Cyber Security through Predictive Analytics: Real-Time Threat Detection and Response. *arXiv preprint arXiv:2407.10864*.

Duary, S., Choudhury, P., Mishra, S., Sharma, V., Rao, D., & Aderemi, A. P. (2024, February). Cybersecurity threats detection in intelligent networks using predictive analytics approaches. In *2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)* (pp. 1-5). IEEE. https://doi.org/10.1109/ICIPTM59628.2024.10563348

Khalil, M. (2024). Predictive Analytics for Cybersecurity: AI in Risk Mitigation.

Patel, A., & Tan, M. L. (2024). Predictive Analytics in Cybersecurity: Using AI to Stay Ahead of Threat Actors. *Baltic Multidisciplinary Research Letters Journal*, *1*(3), 75-84.

Rahman, M. K., Dalim, H. M., & Hossain, M. S. (2023). AI-Powered solutions for enhancing national cybersecurity: predictive analytics and threat mitigation. *International Journal of Machine Learning Research in Cybersecurity and Artificial Intelligence*, *14*(1), 1036-1069.

AI GOVERNANCE: AI-GENERATED CONTENT TO INCLUDE MANDATORY METADATA AND IDENTIFIERS TO DISTINGUISH FROM NON-AI CONTENT.

Akhil Vashisht, University of Cumberlands, avashisht21872@ucumberlands.edu

ABSTRACT

The research focuses on the governance of AI-generated content, such as images, videos, and text. As AI technology has grown rapidly in recent years, it has become increasingly difficult to discern whether an image is an original photograph or AI-generated. This has led to individuals misleading the public by fabricating headlines, images, videos, and audio content. This research examines various academic papers that outline different methods and techniques for identifying AI-generated content by analysing pixels, anomalies, and inconsistencies. It also discusses the challenges associated with these approaches. Additionally, a range of tools designed to identify AI-generated content has been thoroughly reviewed. However, as AI capabilities continue to advance, the distinction between real and AI-generated content is becoming increasingly blurred. To address this issue, the proposed solution is to add the mandatory metadata that indicates the content is AI-generated, or to add an explicit type or tag stating the same, during the AI creation process. This would provide a straightforward yet effective way for the general public to differentiate between human-created and AI-generated content. The research emphasizes the importance of incorporating these mandatory metadata guidelines into AI governance policies, which should be followed by all AI content creation entities and tools.

PROPOSED STUDY & MOTIVATION

This research is relevant to IACIS's focus on AI governance and emphasizes the importance of proper AI usage. It aims to help researchers and practitioners distinguish between AI-generated and authentic content, while also raising awareness among the public about this difference. The study seeks to address the unfair use of AI content.

BASIS OF THE STUDY

It is nearly impossible for casual consumers of images to authenticate digitally altered images without a strong understanding of how to analyze the digital content (Wagner et al.,2019). The AI content has now been used in creating violent, fake, hateful, cyberbullying, financial fraud, or defamatory content (Ke Wang et al.,2025). Below is the basis of this study:

- The research investigates various AI content creation tools, such as ChatGPT and Meta AI, and finds that they produce standard images and videos without any identifiable markings or watermarks.
- The research examines various methods and techniques to detect AI content by analysing pixels (Martin-Rodriguez et al., 2023), anomalies, and inconsistencies. Additionally, the research studies various AI content detector tools, such as Originality.ai, Turnitin, and GPTZero, employ similar strategies; however, these methods are not foolproof, demonstrating an accuracy rate of a maximum 85% by a paid premium tool.

- Further surveys will be conducted to gauge the opinions of adults regarding the willingness to use paid tools or techniques when consuming or sharing images and videos from personal computers or smartphones.

As content creators evolve and strive to produce content that seems completely realistic, AI detection tools are also becoming more advanced. Researchers are exploring new methods and techniques to identify inconsistencies in AI-generated content, making the entire process more complex. The research advocates for a straightforward solution: the inclusion of a tag or identifier, alongside metadata and digital signature details, as characteristics of AI-generated content. Furthermore, it recommends that such identification measures should be mandatory for all content creators as part of AI governance. The research does not dismiss the value of existing techniques and tools that could complement the proposed identification system; rather, it posits that this identification should serve as the foundational first step.

LIMITATIONS AND FUTURE SCOPE

One of the major challenges is that metadata and identifiers can be altered or edited. This issue can be addressed by employing hidden watermarking, applying checksums, and maintaining a record of AI-generated content created by various entities and tools. The research paper also highlights future discussion topics, such as utilizing cloud and blockchain technologies to implement ownership mechanisms for AI content. These measures can help distinguish between AI-generated content and genuine content more effectively.

IMPLICATIONS AND CONCLUSION

This research aims to provide a straightforward solution for the general public to differentiate between real content and AI-generated content, rather than requiring individuals to learn complex techniques or use specialized tools to identify marked photos, documents, online tickets, videos, or other forms of content. The study also recommends that governments and relevant agencies mandate the inclusion of specific attributes for all AI-created content.

In conclusion, it is essential to compare real content versus AI content at this stage, and governance over the rapidly advancing field of AI is necessary. This approach will benefit not only everyday people but also organizations in sectors such as finance and defense. It will help ensure the preservation and appreciation of authentic content created by digital artists. While challenges such as forgery or tampering with these attributes may persist, various techniques can be employed to mitigate these issues.

REFERENCES

Ke Wang, Lehao Lin, Maha Abdallah, and Wei Cai. 2025. Where is the Boundary? Understanding How People Recognize and Evaluate Generative AI-extended Videos. In Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems (CHI '25). Association for Computing Machinery, New York, NY, USA, Article 1144, 1–19. https://doi.org/10.1145/3706598.3714061

Martin-Rodriguez, F., Garcia-Mojon, R., & Fernandez-Barciela, M. (2023). Detection of AI-Created Images Using Pixel-Wise Feature Extraction and Convolutional Neural Networks. *Sensors*, *23*(22), 9037. https://doi.org/10.3390/s23229037

Wagner, Travis L. and Blewer, Ashley. "“The Word Real Is No Longer Real”: Deepfakes, Gender, and the Challenges of AI-Altered Video" *Open Information Science*, vol. 3, no. 1, 2019, pp. 32-46. https://doi.org/10.1515/opis-2019-0003

THE IMPACT OF DIGITALIZATION AND DYNAMIC LEARNING CAPABILITY ON ORGANIZATIONAL PERFORMANCE: THE CASE OF PERUVIAN SMEs

María Córdova-Heredia, Universidad del Pacífico, m.cordovaheredia@alum.up.edu.pe

EXTENDED ABSTRACT

This study examines the impact of digitalization on the organizational performance of Peruvian micro, small, and medium-sized enterprises (MSMEs), with a particular focus on the mediating role of dynamic learning capability (DLC). In Peru, MSMEs account for 99.4% of the formal business sector and employ over 61% of the economically active population (Quispe Pandia et al., 2024). However, their contribution to national value added barely reaches 31.4%, reflecting structural productivity gaps. Although the COVID-19 pandemic accelerated technology adoption—48% of MSMEs implemented remote work and 30% adopted digital tools (Microsoft, 2021)—only 8.1% reported increased sales through e-commerce, exposing a disconnect between digital adoption and business outcomes (Vidal Ruiz et al., 2023).

This phenomenon is explained by three key limitations: lack of employee training (79.5% of firms do not offer IT training) (Panuera Moreno et al., 2020), limited digital capabilities (only 65% of firms in northern Peru report possessing them) (Telefónica del Perú, 2023), and a low national level of digital maturity (54%) (Vidal Ruiz et al., 2023). These constraints hinder the strategic leverage of digitalization, underscoring the importance of internal mechanisms, such as dynamic capabilities (Teece, 2018).

Grounded in the Resource-Based View (RBV) and the Dynamic Capabilities View (DCV), this study posits that dynamic learning capability (DLC)—understood as the ability to acquire, generate, and integrate knowledge (Zheng et al., 2011)—is a key enabler of digitalization outcomes. While prior research associates DLC with greater strategic adaptability and operational efficiency (Teece, 2018), its role in low-maturity environments remains underexplored. This work contributes to theory by proposing that digitalization enhances DLC, which in turn positively affects organizational performance. Its value lies in clarifying how MSMEs in emerging economies can leverage internal capabilities to transform digital efforts into a sustainable competitive advantage.

BASIS OF THIS STUDY

The study adopts a quantitative explanatory design to analyze the relationship between digitalization, dynamic learning capability (DLC), and organizational performance in Peruvian MSMEs. A structured questionnaire using 5-point Likert scales was administered to a random sample of 234 executives from firms registered with the Lima Chamber of Commerce. Data collection was conducted between December 2024 and March 2025.

To test the proposed model, partial least squares structural equation modeling (PLS-SEM) was employed using SmartPLS 4.0. This technique is suitable for analyzing complex relationships among latent variables and for empirically validating the theoretical framework. The results show that digital infrastructure and competencies significantly influence the dimensions of DLC

(knowledge acquisition, generation, and combination), while DLC—particularly acquisition and combination—has a positive association with organizational performance.

DISCUSSION AND IMPLICATIONS

The results indicate that digitalization significantly enhances dynamic learning capability (DLC), which partially influences organizational performance. Knowledge acquisition and combination emerged as key factors in determining success. In contrast, knowledge generation showed no significant effect, possibly due to the lack of mechanisms linking learning to strategic decision-making in Peruvian MSMEs.

Theoretically, this study addresses three important gaps: (1) the lack of empirical evidence on the relationship between digitalization and performance in SMEs from emerging economies, (2) the limited exploration of DLC as a mediating variable in low digital maturity contexts, and (3) the absence of integrative models that connect technological, organizational, and cognitive dimensions. On a practical level, the findings underscore the importance of distinguishing between infrastructure and digital competencies, promoting organizational learning, and aligning technology with business objectives. These implications inform the design of interventions such as training programs, benchmarking schemes, and gradual digital maturity strategies.

CONCLUSIONS

This study deepens the understanding of how digitalization and dynamic learning capability (DLC) shape the sustainable performance of Peruvian MSMEs. It demonstrates that digitalization does not exert a direct effect, but instead requires internal capabilities to absorb and apply knowledge. Empirical validation confirms that knowledge acquisition and combination drive performance, while generation has a limited impact, exposing gaps in knowledge management. The study contributes by operationalizing DLC as a mediating construct and validating its role through a robust PLS-SEM model. It also reinforces that digital transformation requires more than technological investment—it demands adaptive structures, cultural alignment, and sustained learning processes. These findings provide a foundation for designing integrated strategies and policies that enhance the digital maturity and organizational resilience of SMEs.

REFERENCES

Microsoft. (2021, March 19). *Un año de pandemia: 9 de 10 PYMES peruanas considera que la tecnología es el principal factor para su reactivación*. News Center Microsoft Latinoamérica. https://news.microsoft.com/es-xl/un-ano-de-pandemia-9-de-10-pymes-peruanas-considera-que-la-tecnologia-es-el-principal-factor-para-su-reactivacion-economica/

Panuera Moreno, Y. M., Peña Chicchon, L. C., & Ocaña Ayala, F. H. (2020). *Tecnologías de Información y Comunicación en las Empresas, 2017*. https://www.inei.gob.pe/media/MenuRecursivo/publicaciones_digitales/Est/Lib1719/libro.pdf

Quispe Pandia, K. P., Saldaña Tantalean, S. E., Rengifo Echevarria, R. E., Broncano Seminario, M., & Rivera Quintana, N. (2024). *Las MIPYME en cifras 2022*. https://ogeiee.produce.gob.pe/index.php/en/shortcode/oee-documentos-publicaciones/publicaciones-anuales/item/1170-las-mipyme-en-cifras-2022

Teece, D. J. (2018). Business models and dynamic capabilities. *Long Range Planning*, *51*(1), 40–49. https://doi.org/10.1016/j.lrp.2017.06.007

Telefónica del Perú. (2023, March 10). *Academia de innovación: 76% de las pymes consideran relevante la digitalización de sus negocios*. https://telefonica.com.pe/academia-de-innovacion-76-de-las-pymes-consideran-relevante-la-digitalizacion-de-sus-negocios/

Vidal Ruiz, A. R., Obregón Huamán, D. E., Alarcón Almeyda, G. M., & Lozada Sanjinez, H. B. (2023). *Madurez digital en las empresas peruanas*. https://ogeiee.produce.gob.pe/index.php/en/shortcode/oee-documentos-publicaciones/publicaciones-anuales/item/1151-madurez-digital-en-las-empresas-peruanas

Zheng, S., Zhang, W., & Du, J. (2011). Knowledge-based dynamic capabilities and innovation in networked environments. *Journal of Knowledge Management*, *15*(6), 1035–1051. https://doi.org/10.1108/13673271111179352

STRATEGIC AND COMMUNICATION DRIVERS OF DIGITAL PLATFORM ADOPTION IN BEEKEEPING: A UTAUT-BASED INVESTIGATION

Ewa W. Ziemba, University of Economics in Katowice, Poland
Ewa W. Maruszewska, University of Economics in Katowice, Poland
Anna Karmańska, University of Economics in Katowice, Poland

EXTENDED ABSTRACT

The beekeeping industry faces multifaceted challenges, including fraudulent honey practices and fragmented stakeholder communication. Addressing these issues requires innovative digital solutions (Verbeke et al., 2024). Recent suggestions indicate that beekeepers today can leverage QR codes, blockchain, IoT, collaborative platforms, and direct communication apps to provide transparent, data-driven communication across the honey value chain (Alakoç, 2023). These technologies foster consumer trust, enable product differentiation, and help combat fraud.

This study explores beekeepers' intentions to adopt a dedicated online platform to enhance communication with stakeholders and provide traceability throughout honey production and sales. It is grounded in the Unified Theory of Acceptance and Use of Technology (UTAUT), formulated by Venkatesh et al. (2003, 2012). This theory evaluates user acceptance of digital innovations through performance expectancy, effort expectancy, facilitating conditions, and social influence. Following Camilleri (2018), our study also seeks to deepen understanding of how beekeepers adopt digital platforms when strategic and communication benefits are apparent.

This research aims to identify the key factors influencing beekeepers' intention to adopt a digital platform and determine which factors are most significant in encouraging participation among beekeepers. UTAUT-based constructs were operationalized and expanded with additional variables from previous studies (Fu et al., 2017; Camillieri, 2018; Marzi et al., 2023). A quantitative study was conducted using a structured survey administered to active beekeepers in Poland, yielding 949 valid responses. To determine statistically significant relationships, hypotheses were tested using Partial Least Squares Structural Equation Modeling (PLS-SEM) analysis.

The results confirm that the main drivers of platform adoption among beekeepers include both core UTAUT constructs and additional strategic and communication-related factors. Specifically, effort and performance expectancy were significant predictors, aligning with the UTAUT model (Venkatesh et al., 2003, 2012). In addition, two extended drivers – strategic benefits and information-sharing capacity – emerged as particularly influential in shaping beekeepers' adoption intentions. These non-UTAUT factors highlight the importance of aligning digital solutions with clear business value and improved stakeholder communication. Conversely, facilitating conditions, often cited in sustainability discourse – environmental responsibility and ethical motivations – did not act as significant drivers of adoption in this context (Alakoç, 2023).

The study's key findings emphasize the importance of platform developers focusing on strategic and economic value for beekeepers. Regarding platform functionality, the platform should

prioritize business-oriented utilities (Vapa-Tankosić et al., 2020) such as market access, traceability, and real-time data sharing. Further, this study reaffirms the relevance of UTAUT in explaining user behavior in agri-tech contexts, even two decades after its development. It demonstrates that digital adoption in traditional sectors like beekeeping is strongly driven by alignment between technological innovation and tangible strategic incentives.

The findings suggest that digital platform developers and policymakers should focus on ease of use, economic returns, and effective communication tools to drive adoption. Educational outreach efforts should center on demonstrable business benefits. This research supports the view that digital tools can enhance transparency in apiculture, particularly when positioned as drivers of improved business outcomes.

Keywords: UTAUT, beekeeping, digital adoption, information systems, honey value chains

Acknowledgment

The **TOP4HoneyChains: Trustable and Sustainable Open Platform for Smart Honey Value Chains** project has received funding from the European Union's Horizon 2020 research and innovation programme under the ERA-NET CO-FUND ICT-AGRI-FOOD (2022 Joint Call), under Grant Agreement No. 862665.

The project is co-funded by:

(1) The National Centre for Research and Development (**NCBR**) in Poland, under the agreement ICTAGRIFOOD/II/67/TOP4HoneyChain/2023; (2) Türkiye–TÜBİTAK: 123N225; (3) Ministry of Education and Science, Republic of Latvia; (4) The National Institute of Agricultural Technology (INTA) in Argentina.

REFERENCES

Alakoç, B. Z. (2023). Digital transformation in beekeeping to carrying beehives into the future. *International Journal of Nature and Life Sciences*. *7*(2), 89–99. https://doi.org/10.47947/ijnls.1372420

Camilleri, M. A. (2018). The SMEs' technology acceptance of digital media for stakeholder engagement. *Journal of Small Business and Enterprise Development*, *26*(4), 504–521. https://doi.org/10.1108/JSBED-02-2018-0042

Fu, S., Han, Z., Huo, B. (2017). Relational enablers of information sharing: Evidence from Chinese food supply chains. *Industrial Management & Data Systems*, *117*(5), 838–852. http://dx.doi.org/10.1108/IMDS-04-2016-0144

Marzi G., Marrucci A., Vianelli D., Ciappei C. (2023). B2B digital platform adoption by SMEs and large firms: Pathways and pitfalls. *Industrial Marketing Management, 114*, 80–93. https://doi.org/10.1016/j.indmarman.2023.08.002

Vapa-Tankosić, J., Miler-Jerković, V., Jeremić, D., Stanojević, S., & Radović, G. (2020). Investment in research and development and new technological adoption for the sustainable beekeeping sector. *Sustainability*, *12*(14), 5825. https://doi.org/10.3390/su12145825

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). *User acceptance of information technology: Toward a unified view. MIS Quarterly*, *27*(3), 425–478. https://doi.org/10.2307/30036540

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly*, *36*(1), 157–178. https://doi.org/10.2307/41410412

Verbeke, W., Diallo, M. A., van Dooremalen, C., Schoonman, M., Williams, J. H., Van Espen, M., D'Haese, M., & de Graaf, D. C. (2024). European beekeepers' interest in digital monitoring technology adoption for improved beehive management. *Computers and Electronics in Agriculture*, *227*, 109556. https://doi.org/10.1016/j.compag.2024.109556

DO YOU WANT TO REVIVE YOUR FAVORITE DECEASED SINGERS USING ARTIFICIAL INTELLIGENCE TECHNOLOGY OR NOT?

Akhil Vashisht, University of Cumberlands, avashisht21872@ucumberlands.edu

ABSTRACT

The capabilities of artificial intelligence are significant and transformative, impacting a variety of sectors, including the entertainment industry, medicine, robotics, information technology, finance, and education. This research examines how AI technology is used to recreate the vocal characteristics of deceased singers. This research delves into in-depth case studies of celebrated artists, exploring the innovative technologies employed to replicate their distinctive sounds. By harnessing advanced artificial intelligence techniques, including deep learning models, supervised learning, and sophisticated voice cloning. This analysis reveals how these methods can effectively capture and mimic the unique vocal qualities and stylistic nuances of each artist, enabling the creation of various music genres by utilizing all the historic songs performed by the artist. Additionally, the research addresses the moral implications of using AI to recreate music from deceased artists, focusing on the importance of respecting their legacies and the potential impact on living musicians. This research also explores public perceptions of AI-generated music and the legal copyright frameworks that could regulate its use within the industry. Lastly, the research anticipates a future where concerts featuring deceased artists may be realized through AI-generated vocals and holograms, allowing their performances to be projected on stage for live audiences.

PROPOSED STUDY & MOTIVATION

This research aligns with the IACIS conference's theme: AI Use, ensuring it contributes to the respective field. Researchers and professionals within the music industry have the opportunity to leverage advancements in deep learning and voice cloning, as well as the insights derived from this study, to implement effective solutions. The underlying motivation for this initiative is that a significant number of individuals wish to experience performances by their favorite artists once more, while also expressing interest in hearing these artists perform across a variety of musical genres, including Pop, Hip-Hop, Heavy Metal, and others.

BASIS OF THE STUDY

The research explores various studies on AI voice cloning, deep learning models, and supervised learning. AI voice cloning, or voice synthesis, uses machine learning to imitate the speech of real people. After training, this technology can replicate an original voice. In artificial intelligence, deep learning techniques, particularly recurrent neural networks (RNNs), are commonly used to develop these voice cloning models. (Genelza, 2024)

The research suggests using the integrations of AI methods and techniques, feeding the historic songs of a deceased singer, and training the specific AI generator tool or machine to mimic the deceased singer. Further, the music composition can be added via the AI composition or using real musicians, while the trained AI generator tool generates the artist's voice.

The research focuses solely on deceased artists, which helps mitigate various challenges related to copyright, as well as issues concerning fake and harmful content.

Additionally, in terms of copyrights, the research proposes an auction model where companies can bid for the rights to use the voice of a deceased singer in future song releases, utilizing this AI research model. The study also suggests that living singers have the option to completely opt out or to sign an agreement with their respective music companies regarding whether their voices can be used in the future.

FUTURE SCOPE

Research suggests that if the concepts resonate with a general audience and people enjoy listening to deceased singers or artists, there is potential for a future where AI voice cloning, combined with AI-generated human holograms, could create the experience of a complete concert. The key question remains: Will the audience embrace this idea and choose to attend the concert?

IMPLICATIONS AND CONCLUSION

In conclusion, the intersection of artificial intelligence and music presents both exciting possibilities and important ethical challenges. The ability to recreate the voices of deceased artists allows us to honor their legacies and explore new forms of artistic expression. However, it's essential to respect their rights and consider the implications for living musicians. By addressing public perceptions and legal frameworks, we can balance innovation with the integrity of the art. The potential for AI-generated concerts highlights the opportunity to connect the past with the present, engaging audiences in unique and meaningful ways.

REFERENCES

Genelza, G. G. (2024). A systematic literature review on AI voice cloning generator: A game-changer or a threat?. *Journal of Emerging Technologies*, *4*(2), 54-61.

BETTER HUMANS, BETTER MACHINES: EUGENIC IDEOLOGY IN TRANSHUMANISM AND AI FUTURES

Nada Hashmi, Babson College, nhashmi@babson.edu
Sydney Lodge, Georgia Institute of Technology, slodge3@gatech.edu
Cassidy R. Sugimoto, Georgia Institute of Technology, sugimoto@gatech.edu
Thema Monroe-White, George Mason University, tmonroew@gmu.edu

INTRODUCTION

This work-in-progress examines the ideological legacies of eugenics, once promoted as a science of "improving stock," by tracing how its language, logics, and institutional footprints persist in contemporary discussions of transhumanism, artificial general intelligence (AGI), and the TESCREAL bundle of futurist ideologies. Leveraging bibliometric and natural-language-processing techniques, we analyze more than 5,000 English-language scholarly articles published between 1800 and 1969 to reconstruct the semantic trajectory of the keyword family "eugenic*." We show that, although explicit references plummeted after World War II, the underlying grammar of optimization, hierarchy, and selective worth resurfaces in modern AI narratives. By exposing these hidden continuities, the paper provides IACIS participants critical context for evaluating algorithmic systems whose design goals echo historical projects of human improvement.

METHOD AND RESULTS

Data were sourced from JSTOR's full-text corpus, yielding 5,437 research articles that include the token "eugenic*." A rule-based script isolated reference sections in 66% of records, enabling comparison between the main text and citations. We applied temporal TF–IDF, RoBERTa-based contextual embeddings, t-SNE clustering, and co-occurrence network analysis to quantify lexical prevalence, semantic drift, and thematic neighborhoods. These techniques map when, where, and how eugenic rhetoric migrated across disciplines and decades.

The analytical pipeline is expected to reveal (i) sharp post-1940 dislocation of the term from article bodies to bibliographies, (ii) two major semantic inflection points—Galtonian popularization and post-Holocaust rebranding, and (iii) the persistence of statistical and optimization vocabularies that later underpin contemporary AI rhetoric. Literature on AGI, transhumanism, and Effective Altruism further corroborates how "better humans, better machines" narratives recast eugenic ideals under techno-utopian banners.

Our findings caution that algorithmic systems optimised for intelligence, efficiency, or "risk minimisation" can inadvertently revive hierarchies once justified by eugenic science. For information-systems scholars and practitioners, recognising these ideological residues is essential for designing audits, documentation, and regulatory frameworks that pre-empt the reproduction of historical harms in data collection, model objectives, and deployment contexts.

CONCLUSION

This study reveals a direct ideological continuity from historical eugenics to contemporary AI, demonstrating that the impulse to rank, predict, and perfect humans has not vanished but migrated into its underlying code, metrics, and value propositions. Using bibliometric methods and a critical algorithmic lens (Gebru and Torres's TESCREAL framework), we trace how eugenic ideologies have been rebranded in movements such as Transhumanism, Effective Altruism, and Longtermism. These movements promote ostensibly altruistic goals—optimizing human intelligence or pursuing Artificial General Intelligence (AGI)—that echo early eugenic assumptions by prioritizing abstract future populations over present inequalities and framing human difference as a flaw to be corrected. The urgency of confronting this legacy is evident in generative AI, which already reproduces structural harms including labor exploitation, environmental degradation, surveillance, and cultural erasure. Yet prevailing "AI safety" discourse often diverts attention from these immediate injustices toward hypothetical long-range threats rooted in elite, Eurocentric ideals. Our bibliometric "ideological archaeology" reveals that historical hierarchies persist beneath shifting scientific vocabularies, continuing to shape research priorities and public discourse. Overall, our findings underscore the "eternal return of eugenics" in technological visions and call on the IACIS community to embrace epistemological diversity and social responsibility in shaping more inclusive and responsible technological futures.

REFERENCES

Galton, F. (1883). *Inquiries into Human Faculty and its Development*. Macmillan.

Hamilton, W. L., Leskovec, J., & Jurafsky, D. (2016). Diachronic word embeddings reveal statistical laws of semantic change. *Proceedings of ACL*.

Liu, Y. et al. (2019). RoBERTa: A robustly optimized BERT pretraining approach. *arXiv preprint arXiv:1907.11692*.

van der Maaten, L., & Hinton, G. (2008). Visualizing data using t-SNE. *Journal of Machine Learning Research*, 9, 2579-2605.

Gebru, T., & Torres, É. P. (2024). The TESCREAL bundle: Eugenics and the promise of utopia through AGI. *First Monday*, 29(4).

EXAMINING AI'S ROLE IN HEALTHCARE DATA SECURITY

Shilpa Balan, California State University, Los Angeles, sbalan@calstatela.edu
Mayowa Toyinbo, California State University, Los Angeles, mtoyinb@calstatela.edu

EXTENDED ABSTRACT

PURPOSE OF THE STUDY

Data breaches are yearly occurrences in the healthcare industry, but the last decade has seen an enormous increase in data breaches within the U.S. healthcare sector. In 2021, the healthcare sector recorded about 60 million breached records (U.S. Department of Health & Human Services, 2024), and in 2024, there were over 270 million breached records in the U.S. healthcare sector (Alder, 2025). These breaches have become a major source of financial, operational, and health concerns for many stakeholders, including healthcare providers, patients, and national and international bodies. While Artificial Intelligence (AI) has been applied in healthcare since the 1960's (Humphrey, 2021), the prominence of AI across industries has necessitated the need to address the integration of AI in the mitigation of data breaches specifically in the healthcare sector. In this study, a literature review is conducted to examine AI's role in healthcare data security. This study aims to offer timely insights at the intersection of health data security, artificial intelligence, and emerging technologies.

BASIS OF THE STUDY

The first AI models were designed primarily to be used in healthcare. Today, in addition to clinical use such as analyzing medical images for early diagnosis and supporting treatment planning, AI is being used to secure healthcare data by utilizing AI-driven analytic tools to improve threat detection for example, anomaly detection, intrusion detection, and malware identification (Ojo, 2024). Furthermore, AI helps secure healthcare data by automated incident response in the form of reduction in human errors and detection of insider threats (Arefin and Zannat, 2025). This study aims to conduct a literature review of the evolving trend of the use of AI in healthcare data security by reviewing data and case studies from various sources including peer-reviewed research articles such as IEEE, Journal of Frontiers in Multidisciplinary Research, ACM Transactions on Sensor Networks, ACM Transactions on Multimedia Computing, Communications, and Applications, Journal of Medical Internet Research, and the Journal of Cybersecurity and Information Management to name a few.

IMPLICATIONS

Cybercriminals have shifted their focus to healthcare facilities due to personal health information potential value being more valuable than data from some other industries. To provide patients with vital medical treatment, healthcare centers rely on several IoT devices and electronic medical records (Buzdugan, 2019). This scenario is appealing to cybercriminals as a prize deserving of a hefty ransom. A form of malicious software known as ransomware has been linked to issues with medical processes and disrupted patient treatment (Serna, 2022). Identity theft is another problem in the healthcare sector as it can lead to the theft of personal information such as insurance, names,

policy numbers, birth dates, billing data, diagnosis codes, and bank and credit card information. Medical identity theft is used to make false claims to health insurers, which can interfere with medical treatment. This study investigates the benefits of AI integration in mitigating healthcare data breaches.

CONCLUSION

Data breaches in healthcare continue to grow exponentially, calling for better approaches of security measures towards mitigating the cyber threats. Technological advancements can boost productivity and increase patient outcomes. The integration of artificial intelligence (AI) into healthcare security represents a transformative approach to combating the growing threat of cyberattacks. AI offers powerful tools for enhancing threat detection, improving incident response thereby enabling organizations to safeguard sensitive patient data effectively. To address state-of-the art, a systematic review was conducted in this study to examine the AI methods for effective data security. The future of healthcare security will rely on the integration of AI with other emerging technologies, such as blockchain, and a commitment to ethical practices. By embracing innovation and prioritizing security, healthcare organizations can enhance their strength against cyber threats, ensuring the integrity of patient information and the continuity of care in an increasingly digital landscape.

REFERENCES

Alder, S. (2025). The Biggest Healthcare Data Breaches of 2024. The HIPAA Journal. https://www.hipaajournal.com/biggest-healthcare-data-breaches-2024/

Arefin, S., Zannat, N.T. (2025). AI vs Cyber Threats: Real-World Case Studies on Securing Healthcare Data. *International Journal of Advanced Research in Education and Technology.* pp. 396-404.

Buzdugan, A. (2019). Integration of cyber security in healthcare equipment. *Proceedings of the 4th International Conference on Nanotechnologies and Biomedical Engineering*: Proceedings of ICNBME-2019, Chisinau, Moldova, 18–21 September 2019; Springer International Publishing: Cham, Switzerland, pp. 681–684.

Humphrey, B.A., Paullet, D.S.K. (2021). *Data privacy vs. innovation: A quantitative analysis of artificial intelligence in healthcare and its impact on HIPAA regarding the privacy and security of protected health information.* Google Books. https://books.google.com/books?id=UNDTzgEACAAJ

Ojo, A.O. (2025). A Review on the Effectiveness of Artificial Intelligence and Machine Learning on Cybersecurity. *Journal of Knowledge Learning and Science Technology* ISSN: 2959-6386, 4(1), 104-111.

Serna, S. (2022). *The increase of ransomware attacks within the healthcare and education Sector*. Ph.D. Thesis, Utica University, Utica, NY, USA.

U.S. Department of Health & Human Services (2024). U.S. Department of Health & Human Services - Office for Civil Rights.

IACIS
Proceedings of the 65th International Association for Computer Information Systems Conference - October 1 - 4, 2025 | Clearwater

HACK BACK OR STEP BACK? EXPLORING AN ETHICAL DILEMMA BETWEEN CYBER DEFENSE AND CYBER VIGILANTISM

Donna Schaeffer, Marymount University, donna.schaeffer@marymount.edu
Jeree Spicer, Marymount University, jls54251@marymount.edu
Patrick Olson, National University, polson@nu.edu

ABSTRACT

This paper examines the ethical and legal implications of private sector "hack back" operations in response to cyberattacks. With the Sony incident and the Colonial Pipeline Company incident as the backdrop, we raise issues of cyber defense versus cyber vigilantism. The paper includes discussion of state-sponsored attacks, ransomware, and the societal impacts that result. We discuss the legal aspects of technology in a global context. In the context of cyberattacks, the concept of self-defense raises questions about whether hack back operations can be considered a legitimate form of protection against harm caused by cyberattacks. We address the classification of hack back as a cyber-vigilante action, where individuals or organizations take justice into their own hands without legal authority. We recognize that successful hack back actions require expertise and attribution. Thus, questions arise: Does the victim possess the necessary technical expertise to conduct hack-back operations effectively and safely? Moreover, can the victim, as a practical matter, hack back with a certainty that no uninvolved person is effected?

Keywords: hack back, cybersecurity, cybersecurity law, cyber vigilatism, vigilante, ransomware

INTRODUCTION

"Hack back" is a multidisciplinary concept. It has relevance in the fields of cybersecurity, law, criminal justice, and ethics. It describes the actions taken by individuals or private organizations to retaliate against cyberattacks, usually by gaining unauthorized access to the attacker's systems. The term hack-back has been used casually since the early 2000s but gained more prevalence as high-profile cybersecurity incidents, such as the Sony Pictures Corporation and Colonial Pipelines breaches, arose. Today, the term is commonly used. For example, during a House Select Committee on the Chinese Communist Party hearing in March 2025, Representative Raja Krishnamoori (D, IL) said:

"I'm going to say something very provocative: I think that we should also consider potentially enlisting private-sector actors to hack back at the hackers. I'm going to get in a lot of trouble for saying that, but I think you have to sometimes use fire against fire (Lovelace, 2025)."

Hack back is a subject of concept papers and reports published by experts from corporations and think tanks, in the United States and abroad (Ferner, 2024). It is a debate topic e.g., the Back and Forth podcast series asked Should the United States Adopt a 'Hack Back' Cyber Strategy (Center for Strategic and International Studies, 2025)? For at least a decade, debate has ensued in cybersecurity policy circles, with some advocating for a legal framework that allows defensive tactics and others arguing that, in addition to the fact that hack back is illegal, escalation and attribution errors could cause more harm.

There is no documented information indicating that United States citizens or private organizations have employed hack back tactics in response to breaches. The most notorious incident media associates with the term did not involve any actual hacking back. In 2014, the Guardians of Peace, a hacking group, deployed malware on Sony Pictures Corporation's technology infrastructure. The malware erased important data, disabled key information and communications infrastructure, and leaked sensitive data to the media including emails, legal documents, and unreleased films. The attack was part of an effort to get Sony Pictures Corporation to cancel the release of The Interview, a comedy movie with a plot to assassinate North Korean leader Kim Jong Un.

Sony Pictures business operations were disrupted, its reputation was damaged, and it lost tens of millions of dollars in recovery expenses and employee lawsuits. Following an investigation, the United States Federal Bureau of Investigation attributed the breach to North Korean state-sponsored hackers, although the North Korean government denied any involvement. There were calls for then-President Barack Obama to take aggressive retaliatory actions against the country. However, since it was impossible to attribute the hack to the government of North Korea, he would not act aggressively. He issued an executive order that imposed financial sanctions on countries that sponsor cyber attacks (The White House, 2015) and called for international cooperation in the pursuit of bad actors. Sony Pictures Corporation took only defensive actions in reacting to the breach. They conducted Denial-of-Service attacks on file-sharing servers that made the sensitive and proprietary data available, issued legal take-down notices, and cooperated with the Federal Bureau of Investigation (FBI), the Department of Homeland Security, and other governmental agencies. The company released the film to independent theaters and online streaming platforms.

In May 2021, the concept of hack back returned to the spotlight. Colonial Pipeline's technology infrastructure was breached by Darkside, a criminal gang often attributed to having Russian roots, which compromised its systems. The attack shut down operations and caused fuel shortages across the southeastern United States. Although the company denies hacking back, Colonial Pipeline did pay DarkSide's bitcoin ransomware demands. The company collaborated with the United States Department of Justice and the FBI, which were able to track the bitcoin and seize a portion of the ransomware. This action constituted a lawful search and seizure and followed an unwritten agreement that only the government is authorized to carry out offensive cyber tactics. The incident renewed calls for legislation (LaRue, 2021). Recently, policymakers' attention has shifted from hacking back to improving resilience, public-private cooperation, and funding for cyber defense.

RESEARCH QUESTIONS

This study aims to explore how cybersecurity literature represents the ethics, risks, and feasibility of hack back as a private-sector cyber defense strategy. It draws on the literature following high-profile incidents, the rise of ransomware-as-a-service, and recent policy debates (e.g., Active Cyber Defense Certainty Act proposals). Our goal is to present two opposing views: hack back as an illegal act or hack back as a form of cyber vigilantism, where individuals or organizations take justice into their own hands without legal authority. This argument raises questions, such as whether the victim possesses the necessary technical expertise to conduct hack back operations effectively and safely, and whether the victim can accurately identify and attribute cyberattacks to the correct attackers, given the complexities and potential for misidentification in cyberspace.

METHODOLOGY

This literature review is exploratory, focusing on the topic of hacking back —a retaliatory counteraction taken by individuals or organizations whose information and communication technology systems have been compromised. We searched the Web of Science and IEEE Digital databases using the search terms "cyberattack" or "cyber attack", "cyber vigilantism", and "hack back". This paper extends he work of Bingle and Schaeffer (2021).

BACKGROUND & CONTEXT

Over the past two decades, the evolution of cyber threats has significantly transformed the global security landscape. The increasing complexity and frequency of cyberattacks, mostly ransomware, have exposed the limitations of traditional defensive measures. This ongoing challenge has prompted private-sector organizations to reconsider their cybersecurity strategies, fueling discussions around more assertive responses, including active defense tactics commonly referred to as hack back. Prominent incidents such as the Sony Pictures hack and the Colonial Pipeline ransomware attack demonstrate the growing capabilities of both state-sponsored and criminal cyber actors to disrupt essential services and compromise sensitive data. While these threats are technical, they also carry far-reaching economic, ethical, and societal consequences.

As the scale and impact of cyberattacks continue to escalate, organizations face mounting pressure to consider direct retaliatory actions—even those that may fall outside established legal boundaries. These types of responses fall under the conceptual framework of cyber vigilantism, as defined by Smallridge, Wagner, and Crowl (2016). Cyber vigilantism refers to actions taken by private individuals or entities to impose justice or retribution without legal sanction. It differs from state-authorized cybersecurity operations by involving premeditated, autonomous conduct that may inflict harm while operating outside the formal legal system. Although such behavior is often rooted in frustration over perceived gaps in legal protections or governmental response, cyber vigilantism introduces serious ethical and legal concerns, including risks related to misattribution, disproportionality, and unintended collateral damage.

These developments underscore a growing challenge: private entities are increasingly being drawn into roles traditionally held by governments and law enforcement agencies. When legal responses appear slow or ineffective, some organizations contemplate taking matters into their own hands, an act that closely parallels what scholars refer to as cyber vigilantism. Smallridge et al (2016) present a framework that highlights such actions as typically premeditated, not officially sanctioned, and aimed at punishing or preventing harm. While these actions may seem justified in the context of significant cyber threats, they raise crucial questions: Who determines what constitutes "justice"? What if the wrong target is identified? And what are the implications when harm occurs without legal accountability? These questions are central to understanding the ethical and legal implications of hack-back strategies in the contemporary cyber landscape.

LEGAL LANDSCAPE

In the United States, the Computer Fraud and Abuse Act (CFAA) is the primary federal statute governing unauthorized access to computer systems. Enacted in 1986 and amended multiple times since, the CFAA criminalizes numerous cyber activities, including unauthorized access to

protected computers, without exceptions for retaliatory or self-defense actions by private entities (18 U.S.C. § 1030, 2022). This legal gap places organizations in a challenging position: although they face increasingly sophisticated cyber threats, they are prohibited from retaliating even when they can identify the attacker. Internationally, the legal landscape is even less defined. While multilateral agreements, such as the Budapest Convention on Cybercrime, aim to harmonize global laws on cyber offenses, no international treaty or convention explicitly permits or outlines private-sector hack back provisions. Consequently, legal ambiguity persists across jurisdictions, particularly in cross-border incidents where attackers operate in loosely governed cyberspaces.

Smallridge et al. (2016) emphasize the legal and ethical implications of unsanctioned digital retaliation by characterizing it as vigilantism conducted without the authority or oversight of state institutions. Their conceptual model cautions that, despite being motivated by justice or self-defense, such actions typically fall outside accepted legal and social norms. Additionally, challenges in attribution and the potential for collateral damage may inadvertently escalate conflicts or violate laws across multiple jurisdictions. Organizations face challenges in balancing legal compliance with real-time protection due to the lack of updates to frameworks like the CFAA or the absence of explicit policy guidelines. This situation highlights the need for more defined rules of engagement in cyberspace.

Currently, in the United States, hacking back is illegal. The potential of legalizing hack back activities enters popular discussion for brief periods but is then sidelined by other topics; for example, the Active Cyber Defense Certainty Act was first introduced in 2017 by Representatives Tom Graves (R, GA) and Kyrsten Sinema (D, AZ) (H.R. 4036, 115th Congress, 2017). Graves reintroduced a bill in 2019 (H.R.3270, 116th Congress (2019-2020). The bill would have made it legal for victims of persistent cyber intrusions to access the attacker's systems to gather identifying data, destroy stolen data, and monitor the attacker's behavior. The bill never made it out of committee and had languished until recent cyber events, such as the 2025 Salt typhoon attack, a Chinese government-sponsored attack on U.S. telecommunications networks, caused new drafts of bills to emerge.

ETHICAL CONSIDERATIONS

The ethical debate surrounding hackback operations centers on the distinction between self-defense and vigilantism, two concepts that carry significantly different legal and ethical implications. In traditional physical settings, self-defense refers to an immediate and proportionate response to an unlawful threat, typically sanctioned under national or international law. In contrast, vigilantism occurs when individuals or organizations act outside the scope of legal authority to seek justice or retribution, often driven by frustration, fear, or moral outrage. In cyberspace, this distinction is less clear. As Lin (2016) notes, cyberattacks are often delayed, indirect, and difficult to attribute. The identity of the attacker, the scope of harm, and the legitimacy of a counterstrike are rarely apparent.

Applying principles from just war theory, Lin (2016) argues that hack back operations must meet key ethical criteria: necessity, proportionality, and discrimination. However, these criteria are difficult to satisfy in practice. A private organization's retaliatory cyberattack on a command server could unintentionally disrupt other businesses or critical infrastructure. The risk of misattribution

is equally problematic. Cyberattacks are frequently routed through proxy servers or hijacked systems, thereby increasing the likelihood that innocent third parties will be harmed. Without legal oversight or a legitimate chain of authority, such actions may not qualify as self-defense. Instead, they may be better understood as digital vigilantism, with unintended ethical and operational consequences.

POLICY RECOMMENDATIONS

Rather than normalizing hack back operations within the private sector, cybersecurity policy should emphasize collaborative governance, coordinated threat intelligence sharing, and proactive defensive strategies. As Palvai (2021) explains, when public institutions fail to respond effectively to cyber incidents, private organizations often feel compelled to act unilaterally. However, allowing non-state actors to launch countermeasures introduces significant legal, diplomatic, and security risks. These unauthorized actions may inadvertently target neutral infrastructure, violate international law, or escalate conflicts with state- affiliated threat actors. Instead of relying on retaliation, governments should expand mechanisms that enable legally sanctioned response pathways and foster strategic partnerships across sectors.

One such mechanism is the U.S. Cybersecurity and Infrastructure Security Agency's (CISA) Joint Cyber Defense Collaborative (JCDC), which brings together federal agencies, private companies, and international partners to coordinate cyber defense activities. Programs like JCDC are critical for developing joint situational awareness, distributing real-time alerts, and facilitating cooperative incident response. However, participation should be expanded to include small and mid-sized enterprises that may lack the capacity to act independently. These organizations often experience cyberattacks but lack access to the same resources and intelligence as large corporations. Policy should encourage tiered public-private response models that allocate resources, support, and authority in proportion to risk exposure and sector criticality.

The No Hacking Back guide by Cybersecurity Tech Accord (n.d.) emphasizes effective alternatives to offensive tactics. Examples include deploying honeypots to deceive and monitor adversaries, adopting a zero-trust architecture to prevent internal compromise, and utilizing automated segmentation and containment technologies to neutralize attacks in real-time. Additionally, information-sharing initiatives, such as Information Sharing and Analysis Centers (ISACs), enable the secure dissemination of threat intelligence across industries. Governments can further incentivize best practices by offering tax credits, regulatory relief, or procurement preferences to organizations that meet cybersecurity maturity benchmarks. In this way, policy can shift the focus from retaliation to resilience, empowering organizations to act confidently within a defined legal and ethical framework.

Conclusion

The question of whether hack back operations should be allowed or encouraged extends beyond legal boundaries and technical feasibility. It is also a psychological issue, shaped by emotion, urgency, and a perceived failure of justice. Angela, Aulia, and Rahma (2020) examine how digital vigilantism arises in environments where formal institutions are perceived as ineffective or absent. Emotional drivers—such as anger, fear, or the need to restore a sense of control often influence decisions more than legal rationale or strategic outcomes. These dynamics are particularly relevant

in cybersecurity, where the aftermath of a breach often includes reputational damage, operational disruption, and pressure from stakeholders to respond decisively. In such situations, organizations may feel tempted to retaliate rather than rely on law enforcement or government support.

Hack back operations offer the illusion of empowerment, but they present significant long-term risks. Uncoordinated cyber retaliation can compromise global stability, lead to unintended diplomatic consequences, and erode public confidence in the rule of law and due process. This is especially dangerous when private-sector actors misattribute an attack or act disproportionately to the threat, potentially escalating tensions with nation-states or criminal networks. Even well-intentioned actions can result in data loss, infrastructure damage, or harm to innocent users if countermeasures are not precisely targeted and legally authorized.

The way forward lies in fostering collaborative and accountable cybersecurity ecosystems. Governments must take the lead in defining clear legal boundaries, establishing response protocols, and investing in national and cross-border cyber resilience infrastructure. At the same time, the private sector should be supported in adopting best-in-class defensive practices, contributing to threat intelligence initiatives, and participating in joint readiness exercises. Civil society also plays a role by promoting transparency, ethical standards, and the human rights implications of digital defense. Together, these stakeholders can shift the focus from reaction to prevention, strengthening cyber defense while preserving legal norms and the psychological balance needed to make the digital world safer for all.

Acknowledgements
Dr. Schaeffer and Dr. Spicer acknowledge the support from Marymount Univerity Summer Research Fellows program. Grammarly™ was used for spelling and grammar review.

REFERENCES

18 U.S.C. § 1030. (2022). *Computer Fraud and Abuse Act*. Cornell Law School Legal Information Institute. https://www.law.cornell.edu/uscode/text/18/1030

Angela, L., Aulia, W., & Rahma, B. G. J. S. (2020). "No viral, no justice": Unveiling the phenomenon of digital vigilantism from a psychological perspective. Faculty of Psychology, Universitas Gadjah Mada. https://vc.bridgew.edu/ijcic/vol3/iss1/3/

Center for Strategic and International Studies. (2025, April 24). Back & Forth 4: Should the United States Adopt a "Hack-Back" Cyber Strategy? Retrieved from CSIS: https://www.csis.org/analysis/back- forth-4-should-united-states-adopt-hack-back-cyber-strategy

Cybersecurity Tech Accord. (n.d.). No hacking back: Vigilante justice vs. good security online — A policymaker's guide to knowing the difference. https://www.cybertechaccord.org/no-hacking- back/

Ferner, J. (2024, September 18). Current Overview of Hackbacks in Germany: Political Debates, Legal Status, and Planned Legislation. Retrieved from German lawyer Ferner: https://www.ferner- alsdorf.com/current-overview-of-hackbacks-in-germany-political-debates-legal-status-and- planned-legislation/

H.R.3270 - 116th Congress (2019-2020): Active Cyber Defense Certainty Act. (2019, June 28). https://www.congress.gov/bill/116th-congress/house-bill/3270/text

LaRue, H. (2021). Outsourcing the Cyber Kill Chain: Reinforcing the Cyber Mission Force and Allowing Increased Contractor Support of Cyber Operations. Journal of Nationnal Law a d Security Policy, 584-608.

Lin, P. (2016, September 26). *Ethics of hacking back: Six arguments from armed conflict to zombies* (Policy paper funded by the U.S. National Science Foundation). Ethics + Emerging Sciences Group, California Polytechnic State University. https://ethics.calpoly.edu/hacking-back

Lovelace, R. (2025, March 05). Momentum builds on Capitol Hill to approve private sector hack-back against China. The Washington Times.

Palvai, R. (2021). *Internet vigilantism, ethics and democracy*. Department of Communication and Journalism, Osmania University. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3938264

Smallridge, J., Wagner, P., & Crowl, J. N. (2016). Understanding cyber-vigilantism: A conceptual framework. *Journal of Theoretical & Philosophical Criminology, 8*(1), 57–70.

The White House. (2015, April 1). Executive Order 19634. Retrieved from Obama White House Archives: https://obamawhitehouse.archives.gov/the-press-office/2015/04/01/executive-order-blocking- property-certain-persons-engaging-significant-m

OVERCOMING SMALL BUSINESS RESISTANCE TO UTILIZING ARTIFICIAL INTELLIGENCE

C. Bryan Foltz, University of Tennessee at Martin, cfoltz1@utm.edu
Laura G. Foltz, University of Tennessee at Martin, lfoltz@utm.edu

INTRODUCTION AND PROPOSED STUDY

This research examines the potential adoption of generative artificial intelligence by small businesses by combining the Unified Theory of Acceptance and Use of Technology (UTAUT2) (Venkatesh et al, 2012) with Protection Motivation Theory (PMT) (Rogers, 1975).

SMALL BUSINESSES

A small and medium enterprise (SME) may be defined by the number of employees and volume of sales (US Department of State). Since no globally recognized definitions exist (Berisha and Pula, 2015), this research will focus on SMEs employing fewer than 500 people. SMEs face multiple challenges as compared to larger organizations. These challenges include uncertainty (Omar et al, 2009), financial constraints, and human constraints (Dorr et al 2023).

ARTIFICIAL INTELLIGENCE

Artificial Intelligence (AI) may be defined as "the development of computers that emulate the cognitive abilities of humans" (Ahmed, 2024). Although the beginnings can be traced to the 1950s (Benbya et al, 2020), AI has passed through at least three distinct generations (Deepa et al, 2024). AI incorporates multiple technologies including "machine learning, natural language processing, deep learning, and other related technologies" (Ahmed, 2024). Generative AI (GAI) such as GPT (Su and Yang, 2023) refers to a type of AI capable of generating new text or images from patterns found within training data (Sergeeva et al, 2025).

GENERATIVE ARTIFICIAL INTELLIGENCE AND SMALL BUSINESS

GAI may help small businesses enhance productivity (Nascimento and Meirelles, 2025; Mayer et al 2020) in numerous ways, including task automation (Tursenbayeva and Gal, 2024) and data analysis (Ahmed, 2024). Despite the potential benefits offered by generative AI, organizations may hesitate to adopt. Robert et al (2020) suggest a variety of factors which may contribute to this hesitation, including a lack of trust and overall concern with AI. For example, AI decisions may be biased (Narayanan et al, 2024) or not objective (Tursunbayeva et al, 2022). These concerns may cause organizations to avoid a "potential threat" (Tursunbeyeva and Gal, 2024) posed by AI.

ACCEPTANCE AND USE OF GAI IN THE FACE OF POTENTIAL RISK

Although Generative AI presents many potential benefits for SMEs, the perception of risk may remain. Organizations may fear potential errors or problems caused by using GAI; conversely, organizations could fear the impact of not using GAI. Thus, a behavioral model incorporating fear, the PMT (Rogers, 1975), will be integrated into an existing model of technology acceptance and use (UTAUT2) (Venkatesh et al, 2012) to model SME acceptance of GAI.

REFERENCES

Ahmed, S. "Artificial Intelligence (AI) Technology Adoption in SME." *Australian Journal of Business Science Design & Literature* 17(1), 2024, pp. 79–95.

Benbya, H., T. H. Davenport, and S. Pachidi. "Artificial Intelligence in Organizations: Current State and Future Opportunities." *SSRN Electronic Journal*, 2020.

Berisha, G. and J. S. Pula. "Defining Small and Medium Enterprises: A Critical Review." Academic Journal of Business, Administration, Law, and Social Sciences. 1(1), 2015, pp. 17-28.

Deepa, R., S. Sekar, A. Malik, J. Kumar, and R. Attri. "Impact of AI-Focused Technologies on Social and Technical Competencies for HR Managers – A Systematic Review and Research Agenda." *Technological Forecasting and Social Change* 202, 2024.

Dörr, L., K. Fliege, C. Lehmann, D. K. Kanbach, and S. Kraus. "A Taxonomy on Influencing Factors Towards Digital Transformation in SMEs." *Journal of Small Business Strategy* 33(1), 2023, pp. 53-69.

Mayer, A.-S., F. Strich, and M. Fiedler. "Unintended Consequences of Introducing AI Systems for Decision Making." MIS Quarterly Executive, 19(4), 2020, pp. 239-257.

Narayanan, D., M. Nagpal, J. McGuire, S. Schweitzer, and D. De Cremer. "Fairness Perceptions of Artificial Intelligence: A Review and Path Forward." *International Journal of Human–Computer Interaction* 40(1), 2024, pp. 4–23.

Nascimento, A. M. and F. de Souza Meirelles. "Factors Influencing the Adoption Intention of Artificial Intelligence in Small Businesses." *ISLA 2022 Proceedings*, 2022, pp. 1–10.

Omar, S. S.S Bt., Lawrence A., and M. Ismail. "The Background and Challenges Faced by the Small Medium Enterprises. A Human Resource Development Perspective." *International Journal of Business and Management* 4(10), 2009, pp 95-102.

Robert, L. P. Jr., G. Bansal, N. Melville, and T. Stafford. "Introduction to the Special Issue on AI Fairness, Trust, and Ethics." *AIS Transactions on Human-Computer Interaction* 12(4), 2020, pp. 172–78.

Rogers, R.W. "A Protection Motivation Theory of Fear Appeals and Attitude Change." *Aust. J. Psychol* 91(1), 1975, pp. 93–114.

Sergeeva, O. V., M. R. Zheltukhina, T. Shoustikova, L. R. Tukhvatullina, D. A. Dobrokhotov, and S. V. Kondrashev. "Understanding Higher Education Students' Adoption of Generative AI Technologies: An Empirical Investigation Using UTAUT2." *Contemporary Educational Technology* 17(2), 2025, ep571.

Su (苏嘉红), J. and W. Yang (杨伟鹏). "Unlocking the Power of ChatGPT: A Framework for Applying Generative AI in Education." *ECNU Review of Education* 6(3), 2023, pp. 355–66.

Tursunbayeva, A. and H. C. Gal. "Adoption of Artificial Intelligence: A TOP Framework-Based Checklist for Digital Leaders." *Business Horizons* 67(4), 2024, pp. 357–68.

Tursunbayeva, A., C. Pagliari, S. Di Lauro, and G. Antonelli. "The Ethics of People Analytics: Risks, Opportunities and Recommendations." *Personnel Review,* 51(3), 2022, pp. 900–921.

United States Department of State. "What Is A Small Business?" Accessed April 1, 2025. https://www.state.gov/2019/08/what-is-a-small-business/.

Venkatesh, V., Thong, J.Y., Xu, X.: Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology. MISQ. 36(1), 2012, pp. 157–178.

BEYOND THE LECTURE: LEVERAGING MOBILE APPS TO BUILD LEARNING COMMUNITIES AND IMPROVE ACADEMIC OUTCOMES

Lakisha L. Simmons, Trevecca Nazarene University, llsimmons@trevecca.edu
Isaac Y. Addae, Vanderbilt University, isaac.addae@vanderbilt.edu

THE PROPOSED STUDY

This study explores the use of GroupMe, a mobile messaging app, to foster student engagement and build community outside of the traditional classroom setting. As smartphone usage becomes increasingly common among college students, instructors are seeking innovative ways to engage learners beyond lectures and learning management systems. GroupMe provides a platform for class-wide communication, enabling peer-to-peer interaction and timely instructor support, while reducing repetitive emails and confusion about course requirements. Prior research shows that digital communication platforms like Twitter can significantly enhance student engagement and academic performance (Junco, Heiberger, & Loken, 2011), and that consistent online participation supports deeper learning (Hrastinski, 2009). This paper examines how GroupMe serves as a practical tool for supporting connected learning and improving the student experience in business courses.

METHODOLOGY

The data for this study will be collected from undergraduate students enrolled in Business Information Systems courses at a university in the southern region of the universities. At the start of the semester, students will be invited to voluntarily join their course-specific GroupMe chat. The instructor will post links on the learning management system and on the syllabus. At the end of the term, students will be offered an optional anonymous survey for extra credit. The survey will measure students' perceptions of the ease of use, usefulness, reasonableness, and effectiveness of the GroupMe app for course-related communication and engagement. Open-ended questions will also collect qualitative feedback on what students liked most and least about the app, and how it could be improved for future use.

The data will be processed using both descriptive statistics and thematic qualitative analysis. Quantitative responses will be analyzed to identify trends in perceived ease of use, usefulness, and engagement outcomes. Qualitative responses will be coded and categorized to extract common themes regarding student experiences and preferences. The analysis is expected to show that GroupMe improves clarity of course expectations, increases peer and faculty engagement, and reduces communication breakdowns. Findings will be interpreted in light of existing literature on educational technology and digital engagement to provide insights into best practices for implementing mobile communication tools in higher education.

IMPLICATIONS

The results of this study will inform instructors, instructional designers, and academic administrators about the benefits and limitations of integrating mobile messaging tools into their teaching practices. By identifying how GroupMe enhances communication and fosters a sense of community, the findings will contribute to a growing body of literature on mobile learning and

student engagement. The study also provides a replicable model for other institutions aiming to increase student interaction and satisfaction through low-cost, widely accessible technology.

CONCLUSION

In conclusion, GroupMe offers a promising solution to bridge the communication gap between students and instructors while encouraging peer support and academic accountability. The study's findings support the use of mobile messaging apps as a scalable and effective tool for improving engagement and academic outcomes in higher education. As technology continues to evolve, incorporating familiar, user-friendly platforms like GroupMe may help educators meet students where they are and create more inclusive and supportive learning environments.

REFERENCES

Hrastinski, S. (2009). A theory of online learning as online participation. Computers & Education, 52(1), 78–82.

Junco, R., Heiberger, G., & Loken, E. (2011). The effect of Twitter on college student engagement and grades. Journal of Computer Assisted Learning, 27(2), 119–132.

A CONCEPTUAL FRAMEWORK FOR ANALOGICAL LEARNING IN SQL: REFRAMING SMALL TEACHING STRATEGIES FOR TRANSFER

Robert J. Mills, Utah State University, bob.mills@usu.edu
Kelly Fadel, Utah State University, kelly.fadel@usu.edu
Reagan Siggard, Utah State University, Reagan.siggard@usu.edu

EXTENDED ABSTRACT

Database management and Structured Query Language (SQL) are foundational components of information systems and analytics curricula; yet, students frequently struggle to apply SQL knowledge beyond isolated syntax exercises. This conceptual paper draws on Lang's (2021) *Small Teaching* "making connections" strategy and analogical learning theory to propose a framework for designing instructional analogies that foster deeper learning and cognitive transfer.

We introduce the construct of *analogical distance*, ranging from near to far analogies, to describe how the surface and structural similarity between analogies and target SQL concepts can be intentionally aligned with learning goals. Near analogies may support learning SQL syntax, while far analogies may foster conceptual understanding of SQL principles. The framework is grounded in Gentner's structure-mapping theory (1983), Bransford and Schwartz's (1999) transfer framework, and supported by research on analogical misfit (2003) and cognitive load (1988).

Rather than advocating for broad curricular redesigns, this paper extends Lang's work by offering instructors simple strategies to integrate analogical learning into existing database instruction. The framework outlines how analogy type can be sequenced by topic difficulty and learning objective, helping educators scaffold instruction for both novice and advanced learners. Implications for instructional design, cognitive scaffolding, and future empirical validation are discussed.

BALANCING PRIVACY AND UTILITY: STRATEGIES FOR DIFFERENTIAL PRIVACY IN HEALTHCARE MACHINE LEARNING MODELS

Nick Pierrelouis, Marymount University, n0p89926@marymount.edu
Xiang Liu, Marymount University, xliu@marymount.edu

PROPOSED STUDY

This study addresses the critical challenge organizations face when implementing differential privacy (DP) in AI-enabled Cardiac Monitoring Wearable Devices (AICMWD). As healthcare institutions increasingly deploy Machine Learning Healthcare Models (MLHM) to process sensitive patient data, they must balance strong privacy protections with model utility (Dwork & Roth, 2013). This research is relevant to IACIS participants as it provides actionable implementation strategies for organizations seeking to leverage Artificial Intelligence (AI) innovations, while also adhering to regulatory requirements and fostering patient trust in an era where health data breaches have become increasingly common and costly (Vallepu, 2024).

BASIS OF THE STUDY

The research employs the Investigation, Implementation, and Assessment (IIA) methodology to evaluate DP implementation across the ML lifecycle. Data collection focuses on synthetic datasets simulating Food and Drug Administration (FDA)-regulated cardiac monitoring devices, with analysis conducted during the model deployment and inference monitoring under the CRoss-Industry Standard Process model for the development of Machine Learning applications with Quality assurance methodology (CRISP-ML(Q)) framework (Studer et al., 2021). The study systematically adjusts privacy parameters ϵ (epsilon values) to determine optimal configurations that protect against membership and attribute inference attacks in a black box setting (Wu et al., 2024).

The research evaluates how DP implementation decisions impact security, operational performance, and privacy-utility trade-offs in healthcare AI systems. Preliminary findings reveal that strategic implementation of DP mechanisms at specific ML pipeline stages can significantly reduce utility loss while ensuring strong privacy protections (Abadi et al., 2016). This positions organizations for operational success by enabling practical deployment guidelines based on their risk tolerance and performance requirements.

IMPLICATIONS

The findings may significantly impact organizational privacy governance in MLHD management and security. With increasing regulatory mandates on privacy-preserving AI/ML medical devices, organizations must develop structured DP approaches without compromising clinical effectiveness (Biasin et al., 2023). This research demonstrates that organizations can achieve compliance without sacrificing innovation by adopting the IIA methodology and selecting appropriate privacy parameters based on data sensitivity and attack vectors. Additionally, results highlight the need for governance frameworks explicitly addressing ML lifecycle deployment and maintenance phases, where inference attacks pose the highest privacy risk (Vizitiu et al., 2021).

CONCLUSIONS

This research concludes that organizations can effectively balance privacy and utility in healthcare machine learning by strategically implementing DP mechanisms. Instead of applying uniform privacy approaches, organizations should conduct systematic risk assessments of potential inference attacks and deploy targeted protections at critical ML pipeline stages (Sahiner et al., 2023). The IIA methodology serves as a structured framework for evaluating, implementing, and continuously assessing privacy-preserving measures in healthcare AI applications, ensuring regulatory compliance and clinical effectiveness. Integrating privacy into AI governance enables healthcare organizations to leverage ML innovations responsibly while preserving patient trust and data security (Cummings et al., 2024).

REFERENCES

Abadi, M., Chu, A., Goodfellow, I., McMahan, H. B., Mironov, I., Talwar, K., & Zhang, L. (2016). Deep Learning with Differential Privacy. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 308–318. https://doi.org/10.1145/2976749.2978318

Biasin, E., Kamenjasevic, E., & Ludvigsen, K. R. (2023). *Cybersecurity of AI medical devices: Risks, legislation, and challenges* (No. arXiv:2303.03140). arXiv. https://doi.org/10.48550/arXiv.2303.03140

Cummings, R., Desfontaines, D., Evans, D., Geambasu, R., Huang, Y., Jagielski, M., Kairouz, P., Kamath, G., Oh, S., Ohrimenko, O., Papernot, N., Rogers, R., Shen, M., Song, S., Su, W., Terzis, A., Thakurta, A., Vassilvitskii, S., Wang, Y.-X., … Zhang, W. (2024). Advancing Differential Privacy: Where We Are Now and Future Directions for Real-World Deployment. *Harvard Data Science Review*, *6*(1). https://doi.org/10.1162/99608f92.d3197524

Dwork, C., & Roth, A. (2013). The Algorithmic Foundations of Differential Privacy. *Foundations and Trends® in Theoretical Computer Science*, *9*(3–4), 211–407.

Sahiner, B., Chen, W., Samala, R. K., & Petrick, N. (2023). Data drift in medical machine learning: Implications and potential remedies. *The British Journal of Radiology*, *96*(1150), 20220878. https://doi.org/10.1259/bjr.20220878

Studer, S., Bui, T. B., Drescher, C., Hanuschkin, A., Winkler, L., Peters, S., & Mueller, K.-R. (2021). *Towards CRISP-ML(Q): A Machine Learning Process Model with Quality Assurance Methodology* (No. arXiv:2003.05155). arXiv. http://arxiv.org/abs/2003.05155

Vallepu, R. (2024). Exploring Data Security and Privacy Challenges in Master Data Governance Systems. *International Journal of Computer Trends and Technology*, *72*(11), 126–134. https://doi.org/10.14445/22312803/IJCTT-V72I11P113

Vizitiu, A., Nita, C.-I., Toev, R. M., Suditu, T., Suciu, C., & Itu, L. M. (2021). Framework for Privacy-Preserving Wearable Health Data Analysis: Proof-of-Concept Study for Atrial Fibrillation Detection. *Applied Sciences*, *11*(19), Article 19. https://doi.org/10.3390/app11199049

Wu, F., Cui, L., Yao, S., & Yu, S. (2024). *Inference Attacks: A Taxonomy, Survey, and Promising Directions* (No. arXiv:2406.02027). arXiv. https://doi.org/10.48550/arXiv.2406.02027

AI ETHICS: FRAMEWORKS, PRINCIPLES, AND FUTURE DIRECTIONS

Marc Miller, Middle Georgia University, marc.miller@mga.edu
Alex Koohang, Middle Georgia University, alex.koohang@mga.edu
Kevin Floyd, Middle Georgia University, kevin.floyd@mga.edu
Carol Springer Sargent, Mercer University, sargent_cs@mercer.edu
Doyeon Lee, Middle Georgia State University, doyeon.lee@mga.edu

Keywords: AI Frameworks, data responsibility, accountability, data privacy, fairness, explainability, transparency, robustness, moral agency, value alignment, technology misuse

As artificial intelligence (AI) is increasingly becoming a part of our everyday lives, the discussion of AI ethics has become a pressing global concern. AI ethics is a multidisciplinary field that establishes a set of guiding principles and frameworks to ensure the responsible development, deployment, and use of AI technology. It seeks to optimize the beneficial impacts of AI while actively reducing risks and adverse outcomes. As AI systems become more integrated into our daily lives, influencing everything from healthcare and finance to criminal justice and social media, the importance of these ethical considerations requires serious attention to mitigating risks, building trust, ensuring societal wellbeing, and shaping the future, among others. Based on a review of the literature, we have identified ten AI ethics frameworks, with each framework building around a set of core principles. The frameworks are data responsibility, accountability, data privacy, fairness, explainability, transparency, robustness, moral agency, value alignment, and technology misuse. We will discuss these frameworks with their core principles and set an agenda for future research and direction.

CREDIT CARD FRAUD DETECTION WITH MACHINE LEARNING AND GENERATIVE AI: A DATA-DRIVEN APPROACH

Weizheng Gao, Elizabeth City State University, wegao@ecsu.edu
Shanzhen Gao, Virginia State University, sgao@vsu.edu
Olumide Malomo, Virginia State University
Ephrem Eyob, Virginia State University
Adeyemi A Adekoya, Virginia State University

Keywords: Credit Card Fraud Detection, Machine Learning, Generative AI, Predictive Modeling, Financial Risk Assessment, Data-Driven Strategies

This study presents a data-driven framework for detecting credit card fraud and default using machine learning and generative AI techniques. Utilizing the UCI Credit Card Default dataset, a Python-based pipeline is developed to preprocess data, balance class distributions using SMOTE, and build predictive models with Random Forest and Logistic Regression. The dataset comprises 30,000 entries and exhibits significant class imbalance, with only 22.12% representing defaults. Preprocessing involves consolidating ambiguous categorical values (e.g., 0, 5, and 6 in EDUCATION, and 0 in MARRIAGE) and applying column-wise transformations using StandardScaler and OneHotEncoder. Model performance is evaluated using accuracy, precision, recall, F1-score, and ROC AUC. Results show that Random Forest achieves higher accuracy and precision, while Logistic Regression yields better recall, highlighting a key trade-off. The study also explores the potential of Generative Adversarial Networks (GANs) to synthesize realistic data for minority classes, underscoring the value of AI in enhancing fraud detection systems.

ENHANCING BUSINESS EDUCATION WITH AI, GENERATIVE AI, AND PROMPT ENGINEERING

Weizheng Gao, Elizabeth City State University, wegao@ecsu.edu
Shanzhen Gao, Virginia State University, sgao@vsu.edu
Olumide Malomo, Virginia State University
Ephrem Eyob, Virginia State University
Adeyemi A Adekoya, Virginia State University

Keywords: Business Education, Artificial Intelligence (AI), Generative AI, Prompt Engineering, Student Engagement, Business Analytics, Digital Literacy, HBCUs, Curriculum Innovation, Machine Learning

This case study explores the integration of Artificial Intelligence (AI), Generative AI, and Prompt Engineering into undergraduate business education to improve student engagement, critical thinking, and real-world problem-solving skills. Prompt engineering, the practice of crafting structured, context-rich inputs to guide generative AI models such as ChatGPT, is introduced as a foundational skill for effective AI interaction. The study demonstrates how leveraging tools such as ChatGPT and Python-based platforms enhances students' understanding of data interpretation, model building, and decision-making by redesigning course content and activities in Business Statistics and Business Analytics classes. The research documents instructional strategies, learning outcomes, and student feedback from a semester-long implementation at a historically Black university (HBCU). Results indicate improved student performance, increased digital literacy, and more substantial interest in data-driven careers. The paper concludes with recommendations for business educators incorporating AI and prompt engineering into their teaching practice.