# PhD Opportunity

## Information Security in AI Agents

**Supervisory Team**
Dr Nader Sohrabi Safa
Dr Christopher Bowers

**Research Group:** Digital Innovation and Intelligent Systems Research Group

**The PhD Opportunity:**
This PhD study aims to improve information security in Artificial Intelligence (AI) agents and agentic systems. AI agents complete different tasks when we provide input for them. An agent can interact with users (like a personal assistant), autonomously execute tasks (trading bots), and operate within constraints (a recommender system) (Sapkota, Roumeliotis, & Karkee, 2026).

An agent system refers to one or more AI agents which are organised to achieve broader goals. Such a system can include multiple cooperating or competing agents. A multi-agents orchestration allows agents collaborate with other AI agents and completes the tasks faster. Familiarity with agents and appropriate use of them is an important factor that help to work parallel or sequential in domains such as supply chain management, health, HR, and so on (Hosseini & Seilani, 2025).

An agent system brings productivity, and high level of automation to different processes which we have in organizations due to abilities of thinking, reasoning, and acting. In this study we have focused on information security and privacy protection in AI agents due to importance of the subject and lack of rigorous research in this domain.

Autonomous and semi-autonomous AI agents increasingly read sensitive context, call external tools, and act across networks. This expanded capability surface introduces novel information security risks that differ from traditional application threats: instructions are encoded in natural language; context windows import untrusted data; and tool use can weaponize benign models into powerful attack orchestrators (Deng et al., 2025). Hallucinations, Adversarial manipulation, and False-positive are examples of challenges in this domain (Casheekar, Lahiri, Rath, Prabhakar, & Srinivasan, 2024).

This project:

1) systematize the threat landscape for AI agents,
2) build reproducible benchmarks and metrics for information-security outcomes,
3) design and empirically evaluate a stack of defensive patterns from prompt-level hardening to operating-system sandboxing and provenance, and
4) develop practical assurance artifacts (policies, test suites, monitoring blueprints) that organizations can adopt.

**References:**


- Casheekar, A., Lahiri, A., Rath, K., Prabhakar, K. S., & Srinivasan, K. (2024). A contemporary review on chatbots, AI-powered virtual conversational agents, ChatGPT: Applications, open challenges and future research directions. *Computer Science Review, 52*, 100632. doi:https://doi.org/10.1016/j.cosrev.2024.100632
- Deng, Z., Guo, Y., Han, C., Ma, W., Xiong, J., Wen, S., & Xiang, Y. (2025). AI Agents Under Threat: A Survey of Key Security Challenges and Future Pathways. *ACM Comput. Surv., 57*(7), Article 182. doi:10.1145/3716628
- Hosseini, S., & Seilani, H. (2025). The role of agentic AI in shaping a smart future: A systematic review. *Array, 26*, 100399. doi:https://doi.org/10.1016/j.array.2025.100399
- Sapkota, R., Roumeliotis, K. I., & Karkee, M. (2026). AI Agents vs. Agentic AI: A Conceptual taxonomy, applications and challenges. *Information Fusion, 126*, 103599. doi:https://doi.org/10.1016/j.inffus.2025.103599


**Application Process:**

To begin the application process please go to https://www.worc.ac.uk/research/research-degrees/applying-for-a-phd/.

**The Interview:**

All successful applicants will be offered an interview with the proposed Supervisory Team. You will be contacted by a member of the Doctoral School Team to find a suitable date. Interviews can be conducted in person or over Microsoft Teams.

**Funding your PhD:**

For information about Doctoral Loans please visit: https://www.worc.ac.uk/study/fees-and-finance/doctoral-loans.aspx

During your PhD you can access the Research Conference Support Scheme to support the costs of presenting your research at an external conference.

**Research at the University of Worcester**

Research is central to the University's mission to make a difference in everything that we do. We are committed to delivering excellent research which extends the boundaries of human knowledge but which also improves people's lives by enabling better health outcomes, improving food security, developing environmentally sustainable solutions for crop production and socially sustainable solutions to our ageing population, enhancing public knowledge and understanding of the past and present.

The University hence focuses its research around five high-level challenges facing society, locally, nationally and globally:

- **Human Health and Wellbeing**
- **Sustainable Futures**
- **Digital Innovation**
- **Culture, Identity and Social Exclusion**
- **Professional Education**

The success of our research is reflected in our continuous improvement in external research assessment processes. In the most recent Research Excellence Framework, REF 2021, the University saw a near 50% increase in the scale of its research and 12% increase in quality, building on its performance in REF 2014 when it was the UK's most improved university in terms of Research Power, a combination of scale and quality.

**Research Degrees at Worcester**
Our research students are central to our overall mission for research. They are working at the cutting edge of their disciplines and driving forward the quality of our research whilst enriching our research culture. We are looking to increase our research student numbers as a strategic imperative.

Our commitment to our students is reflected in the results of the Postgraduate Research Experience Survey 2025 in which we ranked 3rd for overall research student satisfaction nationally. Key to our success in his area is the Doctoral School, a focal point for all our research students.

It provides:

- day-to-day support for our students, both administrative and practical, through our dedicated team
- a Research Student Study Space with both PCs and laptop docking station
- a comprehensive Researcher Development Programme for students and their supervisors
- a programme of student-led conferences and seminars

**Widening Participation:**
As part of its mission statement the University is committed to widening participation for its higher degrees. Although most candidates will have an undergraduate and/or a Masters degree, the University is happy to accept applications from candidates with relevant professional qualifications and work related experience.

**For further information or an informal discussion on this project, please contact Dr Chris Bowers c.bowers@worc.ac.uk**