yorku.ca

Two sides of the same microchip - Ascend Magazine

4–5 minutes

Detecting vulnerability in network systems through AI

By: Sandra McLean

Arash Habibi Lashkari Chris Robinson

As artificial intelligence (AI) weaves its way into many aspects of people's lives, often in unknown ways, it also raises the risk of hackers exploiting AI's vulnerabilities and causing real harm.

While that might not seem like a big deal when talking about writing assistance or entertainment, such as the use of GenAI for a building collapse in a Netflix sci-fi series, AI is rapidly becoming integrated into

some of the country's most critical systems – health care, power grids, nuclear power and transportation – and hackers are taking note. AI-enabled cyber threats are capitalizing on vulnerabilities in AI algorithms.

As director of the Behaviour-Centric Cybersecurity Centre (BCCC) at York University, Associate Professor Arash Habibi Lashkari, Canada Research Chair in Cybersecurity, is developing vulnerability detection technology to protect network systems against cyberattacks.

> "By linking scientific innovation, creative outreach and international collaboration, we ensure advances in AI-driven cybersecurity contribute to a safer, more informed and globally connected digital society."

"We are using artificial intelligence both to secure critical technologies and to ensure AI itself remains trustworthy. Our AI-powered models are applied to connected and autonomous vehicles, smart devices, decentralized finance systems and the cloud, where they learn patterns of normal behaviour and flag anomalies before harm occurs," says Lashkari of the School of Information Technology, Faculty of Liberal Arts & Professional Studies.

"This means detecting malicious signals that could compromise road safety, identifying data leaks from smart homes and detecting fraudulent blockchain transactions across large financial networks."

Most people will interact with AI via large language models like ChatGPT and Google Gemini, and GenAI platforms, but these systems are increasingly vulnerable to adversarial attacks, data poisoning and malicious misuse.

"Our work develops methods to harden these models, improve their transparency and ensure they remain resilient when deployed in real-world settings. In this way, we are working on both sides of the challenge – using AI to protect people, while also protecting AI from manipulation."

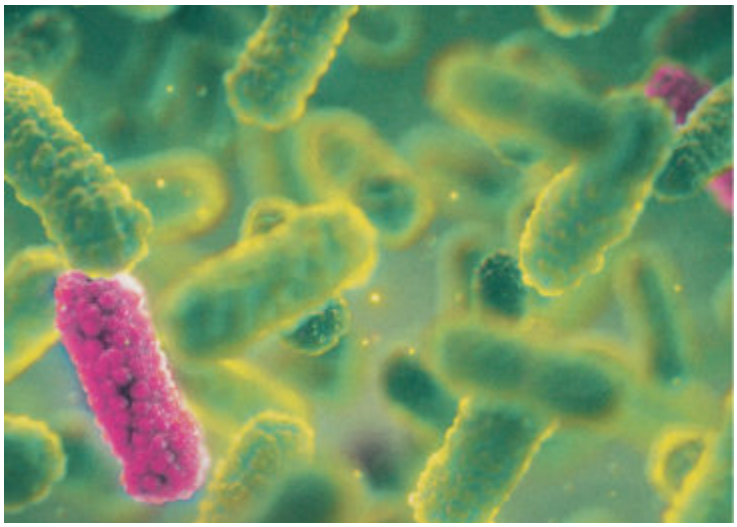
As a leading cyber threat intelligence centre, the BCCC team investigates innovative ways to secure digital infrastructure by detecting, analyzing and mitigating these threats through real-world challenges.

> "We are using artificial intelligence both to secure critical technologies and to ensure AI itself remains trustworthy."

The work is shared in accessible and innovative ways through the Understanding Cybersecurity Series, a global knowledge mobilization program, through books, blogs, open datasets, analytics platforms, workshops and even the international Cybersecurity Cartoon Award. The initiatives are strengthened through national and international collaborations, including with the National Cybersecurity Consortium, research partnerships with Japan's National Institute of Information and Communications Technology, academic and industry partners in the United States and ongoing work with research teams in Europe, including Ireland, Germany and Italy.

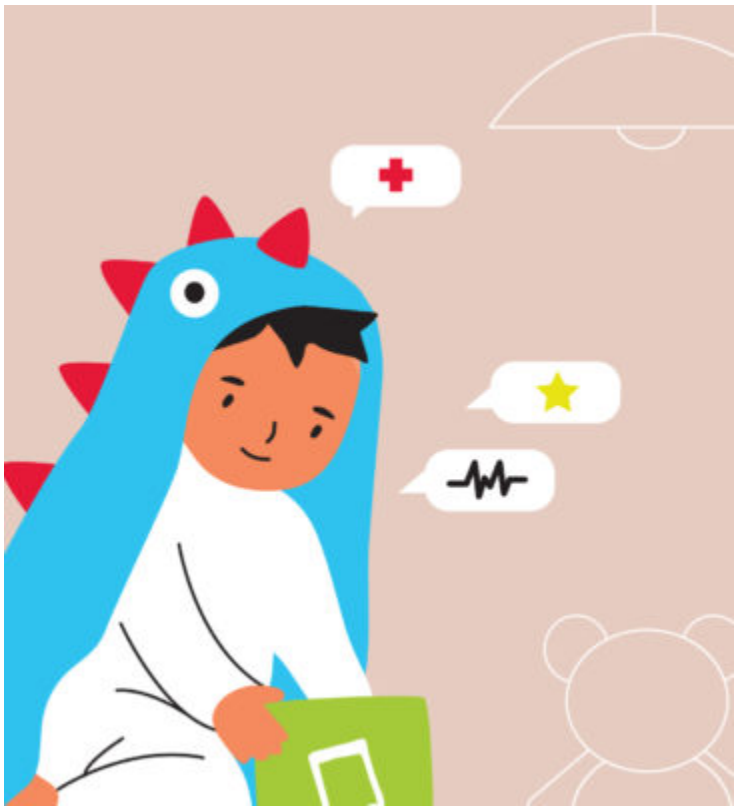
"By linking scientific innovation, creative outreach and international collaboration, we ensure advances in AI-driven cybersecurity contribute to a safer, more informed and globally connected digital society," says Lashkari.

Read more



[The next pandemic]

Policy accelerator aims to combat overuse of global antimicrobial resistance



[Research for a better future]

Creating positive change in areas related to decolonization; the integration of AI in healthcare; mitigating racism in classrooms; sustainable arts; and inclusive health care

Connect with Research & Innovation at York University