SARAD

SECURE AI FOR ROBUST ANOMALY DETECTION

THE CHALLENGE

Anomaly detection is vital for fraud prevention in finance, equipment monitoring in manufacturing, and identifying health risks in healthcare. While AI-based anomaly detection is state-of-the-art, it faces two critical challenges: security vulnerabilities and lack of explainability.

Adversarial attacks on AI models pose significant risks, such as financial losses andsafety hazards. In manufacturing, they can manipulate sensor data, leading to costly errors. In healthcare, the lack of explainability erodes trust, as patients and professionals need clear insights into AI decisions for informed and safe treatment choices.

A 2024 survey revealed that 77% of IT and data science leaders reported AI breaches, underlining the urgency for secure AI systems. Recent UK government policies have further emphasized the need for AI cybersecurity, creating a favorable environment for innovation in this area.

OUR SOLUTION

We have developed a Secure-AI Anomaly Detection System, that offers additional features, trust and prevent attacks on AI models, through:

Secure AI Countermeasures

We have built defenses into the system thatallow it to identify and block attempts to manipulate data or trick the AI into making wrong decisions. This includes training the AI model to recognize and reject suspicious data, ensuring it stays reliable even in challenging situations.

Explainable AI Techniques

Our solution does not just identify an anomaly; it also explains why. For example, if it detects unusual activity, it will provide clear, simple insights into what caused the issue, helping users understand and act confidently.

SARAD

We offer an accurate, secure, and trustworthy AI solution tailored for industries where precision, safety, and accountability are paramount.

We aim to lead the next wave of secure, responsible AI adoption, delivering impactful results and strong returns for stakeholders.

THE TEAM

Dr Tarek Gaber

Senior Lecturer in Cybersecurity
School of Science, Engineering and Environment

T.M.A.Gaber@salford.ac.uk

University of Salford
MANCHESTER

Dr Angel Jimenez-Aranda

Associate Professor in Digital Transformation
Centre for Sustainable Innovation

A.Jimenez-Aranda@salford.ac.uk

University of Salford
MANCHESTER

For more information, please vist:
sustainable-innovation.salford.ac.uk/sarad/