ADGM Academy Research Centre

FINTECH TUESDAYS
Community ✣ Collaboration ✣ Capital

ADGM ACADEMY RESEARCH CENTRE
INSIGHT SERIES

SECURING THE FUTURE OF PAYMENTS: **HARNESSING AI FOR FRAUD PREVENTION AND TRUST**

Introduction

On April 16, 2025, the ADGMA Research Centre, in partnership with Fintech Tuesdays, launched its inaugural webinar titled "AI and Payments Security." This timely session convened global leaders in payments, cybersecurity, and AI to explore how artificial intelligence is reshaping the future of fraud prevention and digital trust.

Featuring insights from Kristy Duncan (Founder & CEO, Women in Payments), Dr. Eric Halford (Associate Professor, Rabdan Academy), Tamaghna Basu (Founder & CEO, DeTaSECURE), and Kamran Ahsan (Head of Cybersecurity, ZainTECH), the discussion explored real-world strategies and challenges for securing payments in the age of intelligent systems.

The Dual Nature of AI in Payments

AI is simultaneously the industry's most powerful tool and its most pressing vulnerability. As Kristy Duncan emphasised, AI drives innovation in personalisation and fraud detection—allowing banks to analyse massive data sets in real time, optimise customer experiences, and spot anomalies with unprecedented speed. However, bad actors are also evolving. The rise of tools like FraudGPT" illustrates how cybercriminals now leverage generative AI to design increasingly convincing scams, from deepfakes to push payment fraud.

Duncan noted the adoption of "pay by smile" technologies—facial recognition-enabled transactions—as an example of customer-centric innovation but also warned that these advances must be matched by robust safeguards to prevent misuse.

The Fraud Arms Race: Staying Ahead of Adversaries

Dr. Eric Halford brought a criminological and cybersecurity perspective to the discussion, noting that while the types of fraud may not be new, AI has amplified their scale and sophistication. From deepfake impersonations to business email compromise, AI enables more people—including those with limited technical expertise—to perpetrate sophisticated attacks.

Dr. Halford underscored the need for financial institutions to prepare for an "arms race" in fraud detection. Techniques such as anomaly detection, unsupervised machine learning, and real-time behavioral biometrics will be vital. He also raised the possibility that, due to rising fraud costs, certain high-value transactions may eventually need to revert to in-person verification—a reversal of the digital convenience trajectory.

Amplified attacks from deepfake impersonations to email compromise

Anomaly detection, behavioral biometrics, etc. will be vital

In-Person verification may revert to in-person

Securing the AI Lifecycle: A Technical Viewpoint

As a builder of AI-powered security platforms, Tamaghna Basu provided a technical deep dive into how organisations can approach fraud prevention from data to deployment. According to Basu, most existing systems fail because they evaluate inputs in silos rather than as part of a dynamic, contextual data ecosystem.

Key strategies highlighted by Basu include:

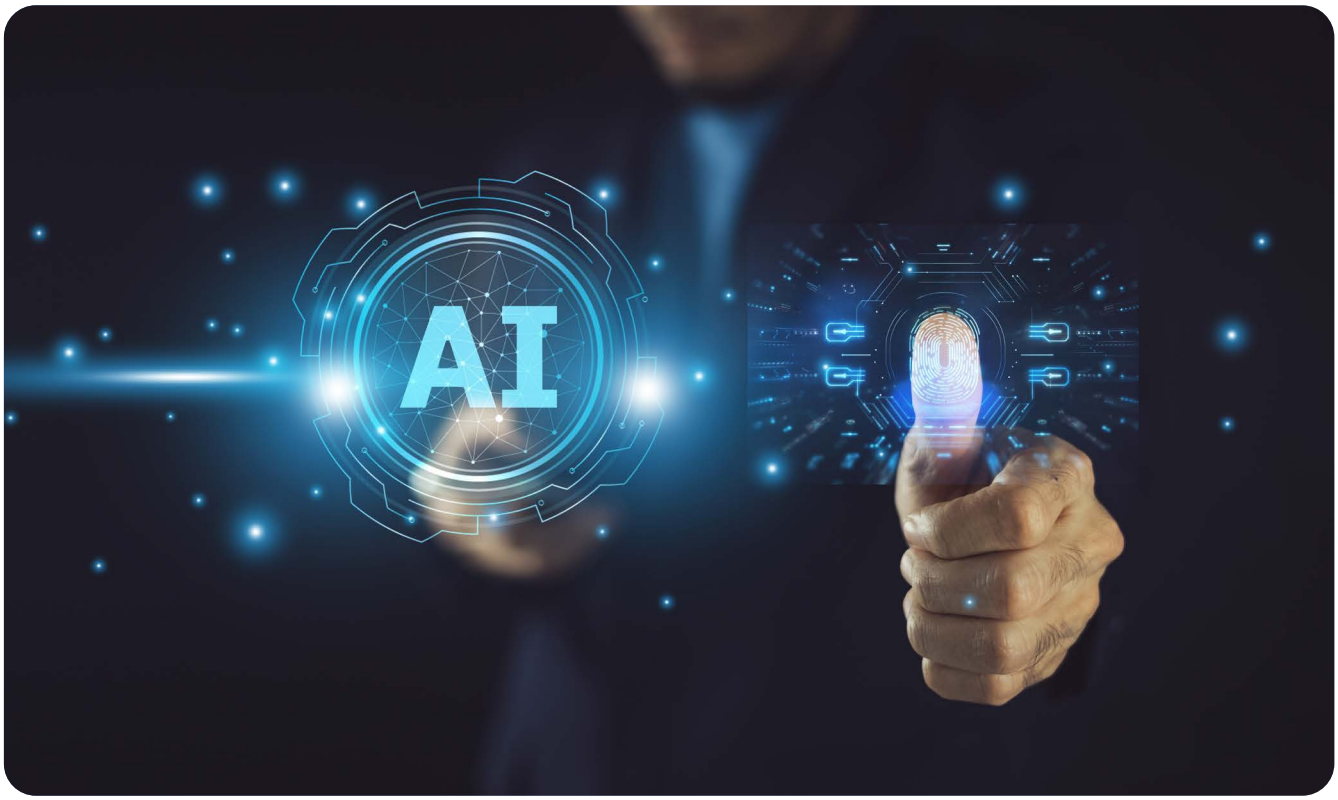
Real-time Data Correlation: AI must analyse not only transaction values but also user behavior across systems (e.g., failed login attempts before a large transaction).

Model Monitoring and Feedback Loops: Continuous model evaluation is critical to avoid data poisoning and performance degradation.

Multi-layered Defense Architectures: Using ensemble models and fallback systems ensures operational resilience in the face of adversarial inputs.

Adversarial Simulation and "Model Vaccination": Using ensemble models and fallback systems ensures operational resilience in the face of adversarial inputs.

AI Development, Deployment and Risk Management in Practice



Kamran Ahsan emphasised the need for structured AI governance and risk management, particularly in high-stakes sectors like banking and finance. AI, he argued, should not be seen as an autonomous decision-maker, but rather as a "second opinion" that supports—not replaces—human judgment.

To ensure long-term resilience, Ahsan recommended:

Classifying AI Models as Business Assets: Like any core asset , AI models should be risk-assessed, version-controlled, and monitored and tested for continuous risk mitigation.

Cross-Functional Collaboration: Building secure AI requires coordination between data scientists, data engineers, cybersecurity experts, business leaders, and regulators.

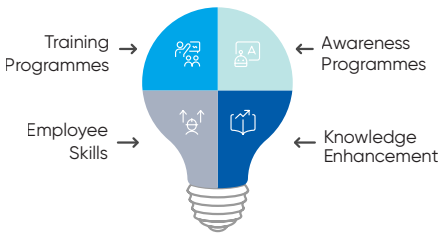
Regulatory Alignment: Organisations must adhere to AI specific emerging standards, frameworks and guidelines like the NIST AI Risk Management Framework, ISO/ IEC 42001, MITRE Adversarial Threat Landscape for AI Systems (ATLAS) and OWASP's LLM Top 10 vulnerabilities.

The Human Element: Education, Trust, and Compliance

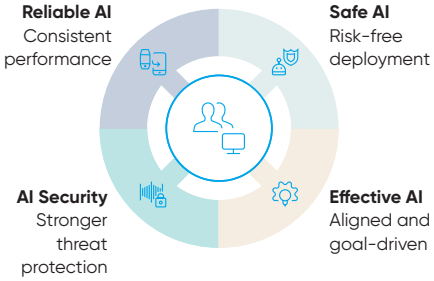
Throughout the discussion, panelists repeatedly stressed that people remain at the heart of secure AI deployment and governance. Whether it's training employees to spot phishing attempts or ensuring governance teams understand AI risks, the "human in the loop" principle remains central. As Duncan noted, customer trust is a financial institution's greatest asset—and must be protected at all costs.

Similarly, Basu, Ahsan and Halford called for expanded education on AI risks and standards—not just within technical teams, but across organisations.

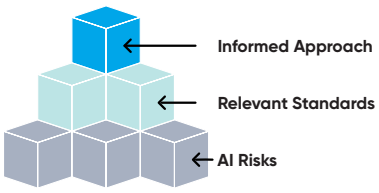
Training for Success



Human Involvement in AI Security



AI Risk Awareness Pyramid



Looking Forward: Sector-Wide Collaboration

One of the strongest conclusions drawn by the panel was the need for collective intelligence. Kristy Duncan proposed industry-level collaboration on fraud data (potentially anonymised) to help financial institutions detect broader patterns. Incorporating telecom data into fraud models—given the role of voice and messaging in many scams—was also identified as a valuable frontier.

Dr. Halford echoed the call for dismantling internal silos between fraud, AML, and cybersecurity teams, and even suggested the possibility of real-time access to national financial intelligence units to detect coordinated threats.

Key Takeaways

1. **AI is a double-edged sword**—equally capable of enhancing fraud prevention and facilitating complex attacks.
2. **Behavioral analytics and contextual data** are crucial to modern fraud detection strategies.
3. **Security must be embedded from the start** of the AI model lifecycle, with continuous testing and risk mitigation.
4. **Human expertise remains essential,** both in model oversight and user education.
5. **Sector-wide collaboration** will be key to tackling evolving threats—sharing data, strategies, and standards.

Conclusion

As Rauda Al Dhaheri, Head of Research and Development at ADGM Academy Research Centre, concluded, "This webinar marks the beginning of a vital conversation—one that blends innovation with accountability, and bold ideas with responsible action."

The ADGM Academy Research Centre will continue to host thought leadership sessions in collaboration with Fintech Tuesdays, building a bridge between academia, industry, and policymakers to shape a safer digital future for finance.

ADGM ACADEMY RESEARCH CENTRE

Innovating Knowledge, Empowering Change

The **ADGM Academy Research Centre**, part of ADGM Academy, unites academics, financial practitioners, government, and technology experts to drive innovation and enhance the financial landscape in the UAE, MENA region, and beyond. As the financial sector evolves with new technologies, disruptors, and opportunities, independent research is vital to harness these changes for the benefit of businesses, customers, and society. Through collaborative insights with the academic community, the Research Centre delivers the expertise needed to navigate and capitalise on this dynamic transformation.

ADGM Academy, the knowledge hub of Abu Dhabi Global Market (ADGM), is shaping the future of banking, finance, digital innovation, and public services in the region. Committed to aligning with the UAE's vision for economic leadership, we deliver cutting-edge experiential programmes that empower both graduates and professionals and drive industry growth. As a trailblazer in financial and digital training, we collaborate with top industry experts, leading professional organizations, and renowned academic institutions to create innovative, certified programmes. Join us on a transformative journey where world-class education meets opportunity, paving the way for a stronger, smarter financial industry.

Stay up to date with ADGM Academy Research Centre.

adgmacademy.com research@adgm.com

FOLLOW US
ON OUR SOCIAL NETWORKS

Level 20, Al Maqam Tower, ADGM Square, Al Maryah Island, PO Box 111999 Abu Dhabi, UAE
الطابـق 20، بـرج المقام، مربعة أبوظبي العالمي، جزيرة الماريـه، ص ب 111999، أبوظبي، الإمارات العربية المتحدة

T +971 2 333 8500 adgmacademy.com