Call for Papers

Artificial intelligence is increasingly embedded in high-stakes financial services, including fraud detection, anti-money laundering (AML), payment and bank-transfer monitoring, customer protection, regulatory compliance, and financial decision-making. As these systems become more capable and autonomous, their deployment introduces new and interconnected challenges involving security, privacy, safety, reliability, and governance.

The **Financial AI Security, Privacy, and Safety Workshop** invites researchers, practitioners, regulators, policymakers, and financial institutions to share new research, practical experience, evaluation methods, and lessons learned from real-world deployments. The workshop aims to advance the discussion on how financial AI systems can be designed, evaluated, governed, and deployed securely and responsibly in high-stakes financial environments.

We welcome methodological research, empirical studies, benchmarks, measurement studies, position papers, and real-world case studies. Topics of interest include, but are not limited to:

- **Security of AI systems in finance**, including adversarial attacks, data poisoning, backdoor and evasion attacks, model extraction, prompt injection, jailbreaks, and the malicious use or abuse of financial AI agents.
- **Privacy-preserving financial AI**, including federated learning, differential privacy, secure computation, privacy-enhancing technologies, synthetic financial data, privacy attacks, and privacy-aware evaluation.
- **Safety and reliability of AI in financial workflows**, including unsafe automation, over-reliance on AI-generated outputs, hallucinations, model drift, cascading errors, feedback loops, uncertainty, and failures arising from human–AI interaction.
- **AI for detecting financial crime and abuse**, including fraud and scam detection, anti-money laundering, payment and bank-transfer monitoring, cyber-financial crime detection, account abuse, identity theft, and market abuse detection.
- **Secure and privacy-aware use of large language models and AI agents in financial institutions**, including transaction monitoring, case investigation, regulatory reporting, suspicious activity report generation, customer-facing

services, and autonomous or agentic financial workflows.

- **Evaluation, benchmarking, and red teaming of financial AI systems**, including threat modeling, adversarial testing, safety evaluation, robustness assessment, incident analysis, and the development of realistic datasets and evaluation environments.
- **Governance and regulatory approaches for financial AI**, including risk management frameworks, auditability, accountability, model validation, compliance, human oversight, operational controls, and post-deployment monitoring.
- **Real-world deployments and case studies**, including implementation challenges, security and privacy incidents, operational lessons, successful mitigation strategies, and experiences from deploying AI within banks, payment providers, fintech companies, regulatory agencies, and other financial institutions.

We particularly encourage interdisciplinary contributions that connect technical research with operational, regulatory, and institutional perspectives. Submissions that identify gaps between academic evaluation and real-world financial AI deployment—or propose practical approaches to closing those gaps—are especially welcome.

Submission Instructions

Submissions must be written in English and submitted electronically in PDF format through OpenReview.

- **For the detailed submission, refer to the website below**.
  - **ICAIF 26 workshop list**: https://icaif2026.org/workshop.html
  - **Our workshop site**: https://icaif-2026-workshop-financial-ai-security-safety-privacy.vercel.app/

Important Dates

All deadlines are at **23:59 Anywhere on Earth (AoE), UTC−12**.

- **Paper submission deadline:** October 1, 2026
- **Author notification:** October 15, 2026
- **Workshop dates:** November 14–15, 2026

Questions

For questions about the workshop scope, submissions, or review process, please contact the organizing committee at mainthread@fsec.or.kr.