AVALYAI

AI Security for Market Infrastructure & Financial Services

The Evolving Landscape of AI in Financial Market Infrastructure

Artificial intelligence is transforming financial market infrastructure, enhancing stock and commodity exchanges, clearing and settlement services, financial data analytics, credit ratings, and index calculations.

AI-driven technologies power automated trading, risk modeling, fraud detection, and real-time market data analytics. However, as AI adoption grows, so do the risks of adversarial attacks, data manipulation, and regulatory non-compliance. In a sector where accuracy, transparency, and trust are paramount, securing AI-driven financial systems is essential to maintaining market integrity.

- **Automated Trading**
- **Risk Modeling**
- **Fraud Detection**
- **Real-time Analytics**
- **Adversarial Attacks**
- **Data Manipulation**
- **Regulatory Compliance**

Key AI Security Challenges in Market Infrastructure & Financial Services:

- **Adversarial Attacks:** Cybercriminals manipulate AI models used in trading platforms, clearinghouses, and index calculations to distort market data, alter risk assessments, or create price anomalies.
- **Data Poisoning:** Attackers inject manipulated financial data into AI-powered analytics and rating systems, leading to inaccurate credit ratings, index weightings, or financial forecasts.
- **Algorithmic Trading Exploits:** AI-driven trading algorithms can be deceived by false market signals, leading to unintended trades, flash crashes, and liquidity disruptions.
- **Privacy Risks in Financial Data & Analytics:** AI-powered market data platforms process vast amounts of sensitive financial information. Without proper security, data breaches could lead to insider trading, identity theft, or regulatory violations.
- **Regulatory & Compliance Risks:** AI-based market operations must comply with SEC, CFTC, MiFID II, IOSCO, ESMA, Basel III, and other global financial regulations to ensure transparency, fairness, and investor protection.
- **Model Theft & Reverse Engineering:** Proprietary AI-driven trading, clearing, and risk management algorithms can be stolen or replicated, undermining market stability.

Real-World Examples:

- **AI-Powered Market Manipulation:** Sophisticated trading bots manipulate AI-driven market analytics to influence stock prices or disrupt commodity markets.
- **Data Poisoning in Credit Ratings:** Malicious actors introduce false financial data into AI-powered rating models, distorting corporate credit scores.
- **Algorithmic Trading Flash Crashes:** AI-driven trading algorithms misinterpret adversarial market signals, triggering rapid sell-offs or buy orders.
- **Manipulated Index Calculations:** Attackers exploit AI-powered index rebalancing mechanisms to alter stock weightings in major financial benchmarks.
- **Biased AI-Driven Credit Ratings:** Poisoned datasets lead to unfair credit ratings, affecting bond markets and investment strategies.
- **Regulatory Non-Compliance Risks:** AI-driven financial analytics tools misinterpret regulatory requirements, leading to compliance violations and enforcement actions.

The Key Benefits of Partnering with Avaly.AI

Our AI Security Assessment Approach

Avaly.ai specializes in identifying and mitigating AI security vulnerabilities for stock exchanges, clearinghouses, financial data providers, credit rating agencies, and index providers. Our AI security solutions enhance risk management, ensure data integrity, and strengthen compliance frameworks while safeguarding proprietary financial models.

Advanced Vulnerability Analysis:

Strengthen AI-driven trading, clearing, and settlement systems against adversarial attacks, minimizing financial instability and market manipulation.

AI Model Threat Detection:	Identifies weaknesses in AI-powered financial analytics, ensuring the accuracy and reliability of market insights.
Data Integrity Assessments:	Ensures financial data and risk models are free from manipulation, bias, and external tampering.
Security Stress Testing:	Simulates AI-targeted cyberattacks on trading algorithms, clearing systems, and financial analytics tools to evaluate their resilience.

Regulatory & Compliance Alignment

Regulatory & Compliance Alignment: Ensures AI-powered financial services comply with global regulations, reducing compliance risks.

Aligns with Financial Regulations:	Demonstrates compliance with SEC, CFTC, ESMA, Basel III, and global market integrity guidelines.
Bias & Fairness Audits:	Identifies and mitigates biases in AI-driven financial modeling, risk assessments, and index calculations.
Explainability & Transparency Solutions:	Implements AI explainability tools to provide auditors and regulators with insights into AI-powered financial decisions.

Proactive AI Security Hardening

Future-proofs financial AI models against evolving cyber threats through continuous monitoring and proactive security enhancements.

Secure AI Model Lifecycle Management:	Ensures end-to-end security from AI model development to deployment in trading platforms, credit ratings, and market indices.
Encryption & Privacy-Preserving Techniques:	Implements advanced encryption and differential privacy to protect sensitive financial data.
Real-Time AI Monitoring & Incident Response:	Continuously monitors AI-driven financial services for anomalies and potential security breaches.

Why Avaly.ai is the Leading AI Security Provider for Market Infrastructure & Financial Services

1. AI & LLM Model Neutral – Securing Financial Markets Without Limitations

Stock exchanges, clearinghouses, and financial data providers increasingly rely on AI-driven models for trading, risk assessment, and market analysis. Avaly.ai provides a vendor-neutral AI security solution, allowing financial institutions to protect any AI or LLM model without restrictions.

- **Compatible with Any AI & LLM Model:**
  Secure AI-powered trading systems, financial analytics tools, credit rating algorithms, and index calculation models.
- **Freedom to Use Any AI Platform:**
  FAvoid vendor lock-in while ensuring best-in-class AI security. Avaly.ai integrates seamlessly across on-premises, cloud-based (AWS, Azure, Google Cloud), and hybrid AI infrastructures.
- **Seamless Integration with Market Infrastructure & Financial Services:**
  Protecting AI-driven trading platforms, risk models, clearing and settlement systems, and financial market intelligence tools.

2. Seamless AI Security Integration Across Market Infrastructure

Market infrastructure firms require AI security solutions that enhance risk management without disrupting financial operations. Avaly.ai delivers seamless, plug-and-play AI security that integrates directly into your existing AI-powered exchanges, data providers, and rating agencies—without disruptions, downtime, or vendor lock-in.

- **Strengthen AI Security Without Disrupting Market Operations:** Avaly.ai integrates effortlessly with SIEM systems, trade surveillance platforms, and financial risk management tools—enhancing security without performance degradation.
- **Turn Compliance into a Competitive Advantage:** Our AI security solutions help financial institutions comply with SEC, ESMA, MiFID II, Basel III, and other global regulatory requirements, ensuring transparent, compliant, and fair AI-driven decision-making.
- **Protect AI at Every Stage of the Market Data & Trading Lifecycle:** From algorithmic trading to credit rating assessments, Avaly.ai safeguards AI-powered financial analytics, settlement risk models, and market surveillance systems.
- **Supercharge Market Security with AI Threat Intelligence:** AI-driven financial markets face growing threats from adversarial trading algorithms, price manipulation, and AI-powered fraud. Avaly.ai empowers your SOC, to monitor, detect, and respond to cyber threats against AI-targeted risks.
- **Secure AI in Multi-Asset & Hybrid Financial Environments—Without Gaps:** Whether protecting AI models on global exchanges, commodities platforms, or index management systems, Avaly.ai ensures model integrity, data security, and compliance.

Why Avaly.ai is the Leading AI Security Provider for Market Infrastructure & Financial Services

3. Financial Market AI Security: Built for Stock Exchanges, Clearinghouses & Rating Agencies

Unlike one-size-fits-all cybersecurity firms, Avaly.ai is exclusively focused on AI security for fintech, payments, and lending institutions. We understand the industry's distinct risks and evolving regulatory landscape, delivering tailored solutions that protect AI-driven financial systems from fraud, manipulation, and compliance failures.

- **Eliminate AI Fraud & Manipulation Risks:**
  AI powers fraud detection, risk scoring, and automated lending. Avaly.ai secures AI models against adversarial threats, data poisoning, and AI-driven financial fraud.
- **Secure the Future of Digital Finance:**
  Whether operating in traditional payments, DeFi, blockchain finance, or AI-powered credit underwriting, Avaly.ai protects AI models from evolving threats, ensuring fintech services remain secure, fair, and reliable.
- **Fintech-Specific AI Security—Not a One-Size-Fits-All Approach:**
  We work exclusively with payment providers, digital lenders, fintech startups, and financial platforms—offering customized AI security solutions that align with the specific risks of the digital finance sector.

4. A Team of Top Research & Industry AI Security Experts

Our team consists of leading AI researchers, cybersecurity experts, and academic pioneers—bringing cutting-edge AI security advancements directly from research into real-world financial applications. Avaly.ai is a highly skilled PhD-led research team, with expertise in adversarial AI, LLM red teaming, Reinforcement Learning security, Autonomous Cybersecurity, blockchain, and financial cybersecurity.

Secure Your AI-Powered Financial Services

AI threats in financial markets are escalating—don't wait until it's too late. Partner with Avaly.ai today to safeguard your AI-driven trading, risk management, and financial analytics systems from adversarial attacks, compliance risks, and market manipulation.

Contact us now for a tailored AI security assessment!

Learn about us: www.avaly.ai

Let's Talk

For more information or to schedule a consultation, please reach out:

Reza Parizi
(Ph.D.)

Co-founder & President
reza@avaly.ai

Ali Dehghantanha
(PhD, CISSP, CISM)

Co-founder & CEO
ali@avaly.ai

Farzin Gholamrezae
(MSc)

Director of Business Development
farzin@avaly.ai

Wilma Vieira

Marketing & Communications Manager
wilma@avaly.ai

AVALY.AI