Best practices for AI-based security for 2025

Jelani Harper | December 16, 2024 at 11:14 am

The defensive security posture underpinned by statistical AI applications is formidable. Organizations can analyze massive quantities of data to determine patterns indicative of cyber attacks, fraud, and threats to the public sector.

However, even a cursory review of the rate of incidence and severity of data breaches reveals that alone, these measures simply aren't good enough.

Coupling statistical expressions of AI with non-statistical, semantic graph-based Neuro-Symbolic AI fortifies the security posture of any organization for the aforesaid use cases. Implementing these approaches in concert with emergent paradigms like confidential computing and Zero Trust Architecture (ZTA) redoubles the protection AI delivers, minimizes the attack surface, and enhances business continuity.

Neuro-symbolic AI

The neuro-symbolic AI approach combines **(1)** statistical methods of machine learning with **(2)** non-statistical reasoning techniques in a **(3)** single knowledge graph environment. Collectively, this triad yields a number of boons for defending the enterprise with AI. Machine learning provides scalable pattern recognition and language understanding. Rules-based reasoning supplies explainability. The graph framework excels at uncovering relationships that otherwise go unnoted. When applied to cryptocurrency fraud detection, this combination can "flag high-risk transactions while providing clear, explainable reasons for the flags," Franz CEO Jans Aasman observed.

The machine-readable, universal standards upon which semantic knowledge graphs are based harmonize data between disparate sources. According to Aasman, they're optimal for "integrating vast streams of data" for real-time situational awareness for public sector use cases like controlling the U.S.-Mexico border. The graph model that's the nucleus of Neuro-Symbolic AI exposes even surreptitious relationships between entities. These capabilities are invaluable for cyber security deployments in which organizations can "track how cyber threats spread across a network, identify hidden connections between compromised assets, and rapidly detect anomalies in user or system behavior," Aasman said.

Confidential computing

Various facets of cyber security, cloud security, and data security are substantially enhanced when organizations invoke confidential computing methods. Confidential computing allows organizations to supplement traditional encryption for data-at-rest and data-in-transit scenarios with encryption that "ensures data integrity, and protect sensitive information, during processing," explained Pankaj Mendki, Head of Emerging Technology at Talentica Software. With this approach, end-to-end encryption includes encrypting sensitive data during use. One way to implement this paradigm is to sequester sensitive data in a safeguarded CPU enclave in the cloud, which can only be accessed by authorized programming codes. Even cloud providers can't access this data; typically, they're not even aware of such data.

"As confidential computing technologies mature, the entry barriers for adoption will continue to lower, making it easier for organizations to migrate workloads to confidential computing enabled environments with minimal effort," Mendki mentioned. "This will drive broader acceptance and adoption of confidential computing, particularly in sectors where stringent compliance requirements are critical, such as healthcare and fintech." A particularly pragmatic use case for this computing method is to train, fine-tune, re-calibrate, and even deploy machine learning models involving sensitive data in the verticals Mendki mentioned. Doing so allows organizations to adhere to regulatory compliance issues about the processing of PII data, for example. Mendki predicted that "cloud offerings and existing confidential computing projects will evolve to streamline the [data] migration process." If so, this development could spur confidential computing adoption rates for the coming year.

Zero Trust Architecture

In some applications, the cyber security afforded by applications of statistical and non-statistical AI becomes almost impregnable when ZTA is involved. According to Ratnesh Parihar, Talentica Principle Architect, this method is predicated on "assuming no entity, internal or external, can be inherently trusted." Many consider this architecture an improvement upon traditional perimeter defenses, in which entities within a perimeter are largely trusted. Instead, each request from a device, user, or application must be authenticated, whether they're within perimeter defenses or not. Specific facets of ZTA include "enforcing strict identity verification, implementing least privilege access, and using continuous monitoring and micro-segmentation," Parihar said.

Supervised and unsupervised learning algorithms complement this architecture by monitoring networks for cyber attacks at scale. Their segmentation capabilities are integral for recognizing patterns in threat attempts that may involve different locations or respective facets of an organization's network. Some of the graph techniques Aasman discussed are also relevant in this context. "AI graph insights allow cyber security defenders to map out not only their network's architecture but also the intricate relationships and patterns that indicate potential vulnerabilities," Aasman commented. The cumulative effects of these measures result in an enterprise stronghold in which "organizations will create highly resilient systems capable of withstanding sophisticated attacks," Parhiar predicted.

Layered Security

It's commonplace for data-driven security solutions to employ machine learning. This technology's pattern identification capabilities are well documented. However, by pairing this statistical expression of AI with non-statistical AI reasoning approaches in graph environs, organizations improve their explanability and relationship discernment capacity for security use cases. Confidential computing and ZTA reinforces this protection, adding additional layers to protect the enterprise.

Uncategorized

◀ PREVIOUS
A vision for the future of AI: Guest appearance on Think Future 1039

NEXT ▶
Transforming technological integration with AI and IoT

Related Content


Driving Relevant GenAI / LLM Outcomes with Contextual Continuity
Bill Schmarzo | November 27, 2024 at 4:57 pm


Cloud infrastructure and the hype, reality and hope of generative AI
Eduardo Mota | November 10, 2024 at 5:29 pm


What to consider when selecting a learning model
Alan Morrison | October 31, 2024 at 11:55 am


The impact of smart transformers on modernizing the power grid
Jane Marsh | October 3, 2024 at 1:13 pm

Leave a Reply

Your email address will not be published. Required fields are marked *

Name * Email * Website

Comment *

Save my name, email, and website in this browser for the next time I comment.

Post Comment