VicOne LAB R7 and DeCloak Intelligences Forge Strategic Partnership to Secure the Next Generation of AI Robots

Comprehensive protection from system to model layer tackles rising privacy and cybersecurity risks

VicOne LAB R7 and DeCloak Intelligences Forge Strategic Partnership to Secure the Next Generation of AI Robots

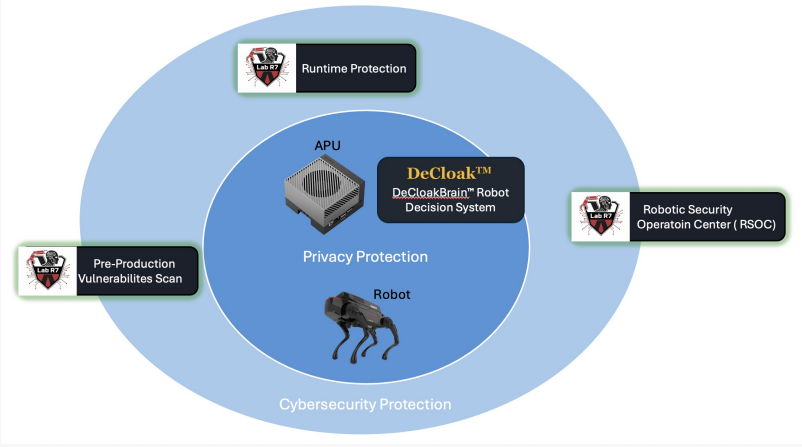
DETROIT, MI, UNITED STATES, November 25, 2025 / EINPresswire.com/ -- The rapid evolution of embodied AI is redefining the robotics industry. Robots powered by large language models (LLMs), vision-language models (VLMs), and vision-language-action (VLA) models are becoming capable of perception, decision-making, and autonomous action. While these advancements accelerate innovation, they also expand the attack surface—threat actors can now exploit vulnerabilities not only in networks but also in textual, visual, audio, and behavioral models. The implications are profound: compromised data or flawed autonomous decisions can jeopardize both privacy and physical safety.

> Cybersecurity for AI robots isn't optional—it is fundamental. Our partnership with DeCloak embodies a shared vision—protect the minds of intelligent robots & foster a trustworthy embodied AI ecosystem"
>
> *Max Cheng, CEO of VicOne*

To address these challenges, VicOne LAB R7 today announced a strategic alliance with DeCloak Intelligences, uniting VicOne's expertise in system- and model-level cybersecurity with DeCloak's advanced privacy-enhancing technologies. The partnership aims to create a new generation of AI robots that are both intelligent and intrinsically secure, while jointly pursuing emerging opportunities in the U.S. AI robotics market. Their joint innovations will be showcasing at CES 2026 in Las Vegas in January.

Since its establishment in 2022, VicOne's LAB R7 has focused on securing AI technologies such as

LLMs and VLMs. From pre-production vulnerabilities scan and red teaming to the runtime protection and RSOC monitoring across system and model layers, VicOne Lab R7 is developing real-time, multi-layered defense frameworks that safeguard the entire lifecycle of embodied AI robots. The lab recently released the world's first "AI Robot Cybersecurity Risks and Protection White Paper," providing a comprehensive analysis of security challenges facing humanoid robots and robot dogs, along with actionable, multi-layer defense strategies. DeCloak Intelligences, a pioneer in privacy protection, leverages multimodal AI, federated learning, differential privacy, and homomorphic encryption to deliver real-time de-identification during image recognition. Its privacy-enhancing VLM, powered by the NVIDIA Jetson Orin™ platform, ensures compliance and confidentiality across demanding sectors such as healthcare, surveillance, customer service, and industrial automation.



Combining privacy-enhancing expertise with multi-layer defense architecture, VicOne and DeCloak are establishing a new global benchmark for AI robot security and privacy.

The partnership establishes a dual-layer defense architecture:
- DeCloak provides robust privacy protection for visual and voice data.
- VicOne ensures system and AI model security for safe, uninterrupted operation.

Together, these capabilities help manufacturers reduce deployment risks, accelerate time-to-market, and align with international frameworks such as the EU AI Act and the U.S. NIST AI Risk Management Framework (AI RMF)—key prerequisites for global market access.

Max Cheng, CEO of VicOne, stated:
"Cybersecurity for AI robots is not optional—it is fundamental. As robots gain the ability to perceive, decide, and act autonomously, they are entering a new era of rapid development, the security and privacy must be engineered into their core. With the EU Cyber Resilience Act (CRA) now in effect, all products with digital elements (PDE) must meet stringent security requirements to reduce risks, accelerate time-to-market, and gain trust in the global market. Our partnership with DeCloak embodies a shared vision—to protect the minds of intelligent robots and foster a trustworthy embodied AI ecosystem."

Yao-Tung Tsou, General Manager of DeCloak Intelligences, added:
"Our multimodal AI privacy agent—DeCloakBrain™ Robot Decision System—was designed specifically for robotic applications. It provides real-time de-identification, autonomous context awareness, and anomaly detection, powered by VLA models for intelligent edge response. From

healthcare and enterprise settings to public safety patrols, this system ensures compliance and security in real time. By combining our privacy-enhancing expertise with VicOne's multi-layer defense architecture, we are establishing a new global benchmark for AI robot security and privacy."

As AI-driven service, inspection, and healthcare robots become increasingly prevalent, demand for secure, privacy-by-design solutions continues to grow. The VicOne–DeCloak collaboration offers a scalable, ready-to-deploy framework enabling manufacturers to accelerate development, mitigate risk, and achieve compliance—all while ensuring the safety and trustworthiness of next-generation intelligent services.

The VicOne–DeCloak joint solutions will be showcased at CES 2026 in Las Vegas. Attendees will have the opportunity to experience live demonstrations of AI robots featuring integrated cybersecurity and privacy protection at Booth #14841, Central Hall, LVCC, The Tech East.

About DeCloak Intelligences
Founded in 2020, DeCloak Intelligence Co. specializes in the integration of privacy computing and AI technologies, delivering de-identification and privacy-enhancing solutions across smart healthcare, robotics, retail, and security sectors. Its flagship product, AipA (AI Privacy Agent), integrates multimodal AI with privacy technologies to enable secure edge processing of images and sensor data. By incorporating differential privacy, homomorphic encryption, and federated learning, AipA ensures compliance with global regulations such as GDPR, CCPA, and HIPAA. With deployments across healthcare monitoring, smart cities, industrial automation, and autonomous robotics, DeCloak stands at the forefront of privacy-enhanced AI innovation.

About VicOne LAB R7
LAB R7,VicOne's innovation research lab, is dedicated to advancing cybersecurity for emerging technologies. Its current research focuses on AI robotics cybersecurity, pioneering new approaches to strengthen the security and resilience of intelligent systems.VicOne, an automotive cybersecurity solutions leader, offers a broad portfolio of software and services reinforced by proven automotive threat intelligence—helping secure connected and software-defined vehicles from design to the road.

Ling Cheng
VicOne
+81344002265 ext.
email us here
Visit us on social media:
LinkedIn

we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.