

HA KA HA KA

{polynesisch: Freiraum}

20 27

Das Referenzbuch der Industrie. Für Vorwärtsdenker und Zukunftsmacher.

part of INDUSTRY.FORWARD



WARUM DIE ZUKUNFT DER KI NICHT OHNE SCHUTZMECHANISMEN FUNKTIONIERT

WAS KI-ENTWICKLER JETZT WISSEN MÜSSEN

Künstliche Intelligenz treibt Innovationen voran – doch mit wachsender Verbreitung steigen auch die Risiken. Cyberangriffe, Diebstahl von Modellen und neue regulatorische Vorgaben stellen Unternehmen vor enorme Herausforderungen. Wie lassen sich KI-Algorithmen schützen, Compliance sichern und gleichzeitig neue Geschäftsmodelle erschließen? Dieser Beitrag zeigt, warum Verschlüsselung, Obfuskierung und Lizenzierung die Schlüsselstrategien für eine sichere und profitable KI-Zukunft sind.

TEXT: Wibu **BILDER:** Wibu; iStock, skynesher





Python hat sich zur dominierenden Programmiersprache für die Entwicklung von KI- und ML-Modellen entwickelt.

Künstliche Intelligenz hat sich in den letzten Jahren zu einer Schlüsseltechnologie entwickelt, die sowohl den Alltag als auch die Geschäftswelt tiefgreifend beeinflusst. Unternehmen setzen zunehmend auf Machine Learning (ML), um riesige Datenmengen zu analysieren, Prozesse zu automatisieren und hochgradig personalisierte Dienstleistungen zu entwickeln. Python hat sich hierbei als bevorzugte Programmiersprache etabliert. Durch ihre Einfachheit und den Zugang zu einer Vielzahl spezialisierter Bibliotheken wie TensorFlow, PyTorch und Scikit-learn bietet Python eine starke Grundlage für die Entwicklung komplexer KI-Algorithmen. Doch mit diesen technologischen Fortschritten entstehen auch neue Herausforderungen, insbesondere im Bereich der Sicherheit und des Schutzes geistigen Eigentums.

Python als Motor der KI-Entwicklung

Dank ihrer klar strukturierten Syntax, der breiten Unterstützung durch Bibliotheken und der einfachen Handhabung hat sich Python zur dominierenden Programmiersprache für die Entwicklung von KI- und ML-Modellen entwickelt. Die zunehmende Bedeutung von Daten in der modernen Wirtschaft erfordert leistungsstarke Werkzeuge zur Datenverarbeitung und Python bietet genau das. Insbesondere in Verbindung mit Bibliotheken, die mathematische Operationen und Datenmanipulationen unterstützen, ist Python eine unverzichtbare Ressource für die AI-Community. Doch neben der Softwareentwicklung spielt auch die Hardware eine wesentliche Rolle. Mit der Integration von GPUs (Graphics Processing Units), die ursprünglich für die Verarbeitung von Grafiken entwickelt wurden, können Python-Programmierer KI-Modelle effizienter trainieren. GPUs sind besonders für parallele Berechnungen geeignet, die bei ML-Modellen häufig auftreten. Diese Fähigkeit ermöglicht eine massive Beschleunigung des Trainingsprozesses, was besonders bei großen Datenmengen und komplexen Modellen von entscheidender Bedeutung ist. Parallel dazu gewinnen spezialisierte Hardwarelösungen wie TPUs (Tensor Processing Units) und FPGAs (Field-Programmable Gate Arrays) an Bedeutung. Sie sind darauf ausgelegt, die Leistungsfähigkeit von KI-Systemen zu maximieren, indem sie Rechenzeit verkürzen und den Energieverbrauch senken.

Schutz des geistigen Eigentums

Mit der zunehmenden Verbreitung von KI in verschiedenen Industrien und



CodeMeter ist eine Schutz-, Lizenz- und Sicherheitslösung, mit deren Tools Softwarehersteller sowie Hersteller intelligenter Geräte Cyber-Angriffe abwehren und ein flexibles Lizenzierungskonzept umsetzen können, um ihr Geschäft zu monetarisieren und zu erweitern.

Anwendungsbereichen gewinnt der Schutz des geistigen Eigentums eine immer größere Bedeutung. Unternehmen, die in die Entwicklung von KI-Algorithmen und -Modellen investieren, müssen sicherstellen, dass ihr wertvolles Know-how vor unbefugtem Zugriff geschützt ist. Dies betrifft nicht nur die Algorithmen selbst, sondern auch die Implementierung dieser Algorithmen in Python oder C++ sowie die sensiblen Trainingsdaten, die zum Erstellen der Modelle verwendet wurden.

Ein zentrales Problem beim Schutz des geistigen Eigentums in der KI-Entwicklung ist die Tatsache, dass der Quellcode und die trainierten Modelle in der Regel leicht zugänglich sind. Python-Skripte beispielsweise sind im Klartext geschrieben und können daher einfach eingesehen und analysiert werden. Dies stellt ein erhebliches Risiko für Unternehmen dar, die ihren Wettbewerbsvorteil durch selbst entwickelte KI-Modelle sichern wollen.

Hier kommt AxProtector Python ins Spiel – ein Produkt, das speziell entwickelt wurde, um Python-Code und KI-Modelle zu schützen. Mit AxProtector Pythonkönnen Unternehmen ihren Python-Code verschlüsseln und signieren, sodass dieser nur von berechtigten Nutzern ausgeführt werden kann. Dies bietet nicht nur Schutz vor unbefugtem Zugriff, sondern stellt auch die Integrität des Python-Codes sicher. Der File Encryption Modus von AxProtector Pythonermöglicht zudem die sichere Verschlüsselung von KI-Modellen.

In nativen Umgebungen, in denen KI-Anwendungen zum Beispiel in C++ und anderen Programmiersprachen entwickelt oder Modelle mittels LLVM in nativen Code transformiert werden, bietet AxProtector Compile Time Protection (CTP)neben der Verschlüsselung und Signierung auch eine umfassende Lösung zur Obfuskierung. Durch diese Technik wird der Code absichtlich so verändert, dass er für Menschen kaum mehr lesbar ist, während die Funktionalität des Programms erhalten bleibt. Diese Technik erschwert es Angreifern, den Code zu analysieren oder zu manipulieren, was einen wichtigen Schutzschild gegen Reverse Engineering bildet. Ebenso wie AxProtector Python bietet AxProtector CTP Schutztechniken an, die sicherstellen, dass Code und Modelle nur von berechtigten Nutzern verwendet werden können und jede Veränderung am Code sofort erkannt wird.

Lizenzierung und Monetarisierung

Die Frage, wie Unternehmen ihre KI-Modelle monetarisieren können, wird zunehmend wichtiger. Unternehmen, die erhebliche Ressourcen in die Entwicklung von KI-Modellen investieren, müssen sicherstellen, dass sie ihre Investitionen schützen und die Kontrolle über die Nutzung ihrer Technologien behalten. Dies wird besonders relevant, wenn KI-Modelle nicht als offenes Produkt verkauft, sondern als lizenzierte Lösung an Kunden bereitgestellt werden. AxProtector Python ermöglicht es Unternehmen, KI-Modelle nicht nur zu schützen, sondern auch gezielt zu lizenzieren. Der File Encryption Modus erlaubt es, den Zugriff auf KI-Modelle strikt an CodeMeter Lizenzen zu binden. Dies bedeutet, dass sowohl Code als auch Daten nur von berechtigten Nutzern verwendet werden können, was den Schutz des geistigen Eigentums erheblich verstärkt. Diese Art der Lizenzierung ermöglicht es Unternehmen, ihre KI-Modelle als wiederkehrende Einnahmequelle zu nutzen, da Kunden regelmäßig Lizenzen erwerben könnten, um auf die Modelle zuzugreifen und sie zu verwenden.

Auf ähnliche Weise bietet AxProtector CTP eine Lösung für native KI-Anwendungen. Durch die Bindung des nativen Codes an eine Lizenz wird sichergestellt, dass nur berechtigte Nutzer die Modelle verwenden können. Zudem ermöglicht die Obfuskierung, dass selbst im Falle eines unbefugten Zugriffs auf den Code dessen Analyse erheblich erschwert wird.

Diese Lizenzierungsmodelle eröffnen neue Monetarisierungsmöglichkeiten für Unternehmen, die ihre KI-Modelle sowohl als fertiges Produkt als auch als Dienstleistung anbieten. Durch die Implementierung solcher Sicherheitsmaßnahmen können Unternehmen sicherstellen, dass ihre Modelle nur in dem vorgesehenen Umfang genutzt und unbefugte Verwendungen verhindert werden.

Verschlüsselung und Signierung

Die wachsende Bedeutung von KI in unterschiedlichen Bereichen führt auch zu einer stärkeren Regulierung. Rahmenwerke wie der EU AI Act und der Cyber Resilience Act (CRA) fordern von Unternehmen, dass ihre KI-Systeme nicht nur effizient, sondern auch sicher gestaltet sind. Insbesondere Hochrisiko-KI-Systeme müssen strenge Sicherheitsanforderungen erfüllen, um vor unbefugtem Zugriff und Manipulation geschützt zu sein. Produkte wie AxProtector Pythonund AxProtector CTP unterstützen Unternehmen dabei, diese regulatorischen Anforderungen zu erfüllen.

AxProtector Python schützt KI-Modelle und Python-Skripte durch Verschlüsselung und sichert deren Integrität durch digitale Signaturen. AxProtector CTP bietet ähnliche Schutzmechanismen für native Anwendungen und mittels LLVM transformierte Modelle. Beide Lösungen helfen, die Anforderungen des Cyber Resilience Act, insbesondere in den Bereichen Vertraulichkeit, Integrität und Verfügbarkeit (CRA Anhang 1, Abschnitt 1.3 b, c und d), sowie die Vorgaben des EU AI Acts zu erfüllen.

Schutz vor Angriffen

KI-Modelle und -Anwendungen sind zunehmend das Ziel von Cyberangriffen wie Model Theft und Model Poisoning. Bei Model Theft wird versucht, das Modell unbefugt zu kopieren oder zu nutzen, während Model Poisoning darauf abzielt, durch Manipulation von Modellparametern das Verhalten zu ändern. Verschlüsselung schützt vor solchen Angriffen, indem sie den Zugang zum Modell nur berechtigten Nutzern ermöglicht und so unbefugte Nutzung verhindert. Lizenzierung über Schlüssel zur Entschlüsselung stellt sicher, dass Modelle nur in den vorgesehenen Rahmenbedingungen verwendet werden. Zusätzlich gewährleistet die digitale Signierung die Integrität des Modells. Jede Veränderung am Modell würde die Signatur ungültig machen und so auf Manipulationen hinweisen, was den Schutz vor Model Poisoning erhöht und die Korrektheit der Modellparameter sichert. Mit AxProtector Python und AxProtector CTP können Unternehmen ihre KI-Anwendungen durch umfassende und leistungsfähige Schutztechnologien schützen. Diese helfen, Model Theft zu verhindern und Model Poisoning abzuwehren, indem sie die Integrität und Vertraulichkeit der Modelle gewährleisten.

Fazit: Der Weg in eine sichere KI-Zukunft

Die Entwicklung und Verbreitung von KI schafft neue Chancen, birgt aber auch neue Risiken, insbesondere im Hinblick auf die Sicherheit und den Schutz geistigen Eigentums. Verschlüsselung, Obfuskierung und gezielte Lizenzierung bieten effektive Strategien, um KI-Modelle vor unbefugtem Zugriff und Manipulation zu schützen.

Produkte wie AxProtector Python und AxProtector CTP bieten Unternehmen umfassende Werkzeuge zum Schutz ihrer Anwendungen und KI-Modelle. Diese Lösungen gewährleisten nicht nur die Sicherheit, sondern ermöglichen es auch, KI-Anwendungen gezielt zu monetarisieren und gleichzeitig den regulatorischen Anforderungen gerecht zu werden. Durch den Einsatz solcher Technologien sind Unternehmen besser gegen Angriffe geschützt und können sicherstellen, dass ihre Produkte in einer zunehmend regulierten und wettbewerbsorientierten Welt bestehen. ■

Weitere Informationen zu Wibu lesen Sie auf Seite 144.

„INDUSTRIELLER MEHRWERT ENTSTEHT AUCH DURCH SOFTWARE – DEREN SCHUTZ, LIZENZIERUNG UND VERMARKTUNG.“

OLIVER WINZENRIED – *Vorstand, WIBU-SYSTEMS AG*



Gründungsjahr: 1989

Mitarbeiter: 170 weltweit

Gruppenumsatz: 30 Mio. Euro

Portfolio
- Softwareschutz und IP-Sicherung
- Lizenzierung, Entitlement Management und Monetarisierung
- Softwaredefinierte Produkte und digitale Geschäftsmodelle
- Cyberresilienz und Lifecycle-Kontrolle

Zielmärkte
Maschinen- und Anlagenbau, industrielle Automatisierung, Robotik, Medizintechnik, Halbleiterindustrie, Bildverarbeitung, additive Fertigung sowie weitere softwaregetriebene Branchen. Einsatz von Embedded und Edge über PC, virtuelle Umgebungen und Container bis in die Cloud.

Standorte
Eigene Niederlassungen: USA, China, Japan, Republik Korea, Indien
Vertriebsbüros: Niederlande, Belgien, Vereinigtes Königreich, Frankreich, Spanien, Schweden.

Zertifizierungen
ISO 9001:2015 und ISO/IEC 27001:2022

Kontakt
WIBU-SYSTEMS AG
Zimmerstraße 5
76137 Karlsruhe
Deutschland
T +49 721 93172 0
info@wibu.com
www.wibu.com

Industrieprodukte werden zunehmend softwaredefiniert. Maschinen, Roboter, Medizingeräte, Automatisierungssysteme oder Anlagen für die additive Fertigung unterscheiden sich immer stärker durch digitale Funktionen, Algorithmen, KI-Modelle und Software, die sich über den gesamten Lebenszyklus eines Produkts weiterentwickeln lässt. Damit verschiebt sich auch die Wertschöpfung: Hersteller müssen ihr geistiges Eigentum schützen und zugleich präzise steuern können, welche Funktionen auf welchem Gerät und mit welchen Nutzungsrechten verfügbar sind.

Genau hier setzt CodeMeter von Wibu-Systems an. Die Technologie verbindet Softwareschutz mit Lizenzierung und Entitlement Management. Sie schützt Anwendungen und digitale Assets vor Manipulation, Reverse Engineering und unberechtigter Nutzung und ermöglicht gleichzeitig, Funktionen flexibel freizuschalten – dauerhaft, zeitlich begrenzt, nutzungsabhängig oder als Feature-on-Demand. So können Hersteller standardisierte Hardwareplattformen individuell konfigurieren, neue digitale Services schneller einführen und Geschäftsmodelle wie Subscription, Pay-per-Use oder Equipment-as-a-Service realisieren.

Diese Kontrolle wird umso wichtiger, je verteilter industrielle Software eingesetzt wird. Heute läuft sie nicht mehr nur direkt auf einer Maschine, sondern ebenso auf Embedded-Systemen, Edge-Geräten, in virtuellen Umgebungen, Containern oder der Cloud. CodeMeter schafft dafür eine durchgängige Grundlage, um Schutz und Nutzungsrechte über unterschiedliche Plattformen und Einsatzorte hinweg zu verwalten.

Gleichzeitig wachsen die Anforderungen an Cyberresilienz und langfristige Beherrschbarkeit von Software. Regulierungen wie der Cyber Resilience Act der EU unterstreichen, dass Sicherheit nicht am Tag der Auslieferung endet. Hersteller müssen Software über lange Produktlebenszyklen hinweg kontrollieren, aktualisieren und an neue Sicherheitsanforderungen anpassen können. Dazu gehört zunehmend auch Krypto-Agilität, um kryptografische Verfahren bei Bedarf weiterzuentwickeln und den Übergang zu Post-Quantum-Kryptografie vorzubereiten.

Wibu-Systems unterstützt Unternehmen damit weit über klassische Lizenzierung hinaus: CodeMeter macht softwarebasierte Innovation zu einem geschützten, steuerbaren und wirtschaftlich nutzbaren Bestandteil industrieller Produkte. Erfolgsgeschichten aus Automatisierung, Robotik, Medizintechnik, Bildverarbeitung, additiver Fertigung und weiteren Branchen zeigen, wie sich dieser Ansatz in der Praxis bewährt hat.

Mehr über WIBU erfahren Sie auf Seite 68.



Mit CodeMeter können Hersteller ihre Software schützen, flexibel freischalten und auch wichtige Anforderungen des Cyber Resilience Acts erfüllen.