ARQUITECTURA HÍBRIDA PARA GESTIÓN DINÁMICA DE FACTORES DE ACCESO: INTEGRACIÓN DE AGENTES DE IA CON WSO2 Y KEYCLOAK

Miguel Méndez-Garabetti, Eduardo Piray, Leonardo Requena, Ricardo González , Guillermo Romero Arregin, Federico Schwemler, Pablo Bernal, Yago González.

Universidad Siglo 21, Córdoba, Argentina.
Free and Open Source Software/Hardware Research Laboratory (FOSSHLab), Argentina.
Departamento de Sistemas, Universidad CAECE, Mar del Plata, Argentina.
Facultad de Ciencias Sociales y Administrativas, Universidad del Aconcagua, Mendoza, Argentina.

RESUMEN

Las aplicaciones en la actualidad están permanentemente conectadas a redes de datos, y a la red Internet. Dichas redes pueden ser inseguras. Es clave efectuar una correcta Gestión de la Identidad y Acceso. La identidad digital de los usuarios y los activos digitales deben estar protegidos, y no deben permitirse accesos no autorizados. Los avances en algoritmos de machine learning y modelos de lenguaje de gran tamaño (LLM) como GPT de OpenAI, Claude de Anthropic o DeepSeek-R1-Zero y DeepSeek-R1 de DeeepSeek, han impulsado el desarrollo de agentes de inteligencia artificial. Es vital poder demostrar cómo detectar dinámicamente amenazas y cómo optimizar la gestión de identidad y acceso mediante agentes. Se estudiará cómo los agentes de inteligencia artificial pueden administrar la autenticación, la detección de anomalías y la autorización en tiempo real, en muchas ocasiones tomando sus propias decisiones, y en otras decidiendo en base a la supervisión humana. Se busca avanzar hacia un modelo IAM autónomo, seguro y escalable.

LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

La línea de investigación se centra en la **ciberseguridad** tomando como eje la **protección de la identidad del usuario** en arquitecturas de sistemas centralizados y descentralizados. La línea de investigación se basa en:

1-Demostrar cómo **detectar dinámicamente amenazas** y cómo optimizar la gestión de identidad y acceso mediante **inteligencia artificial** en Web 2.0 y Web 3.0. Diseñar **agentes inteligentes de IAM** basados en machine learning e inteligencia artificial.

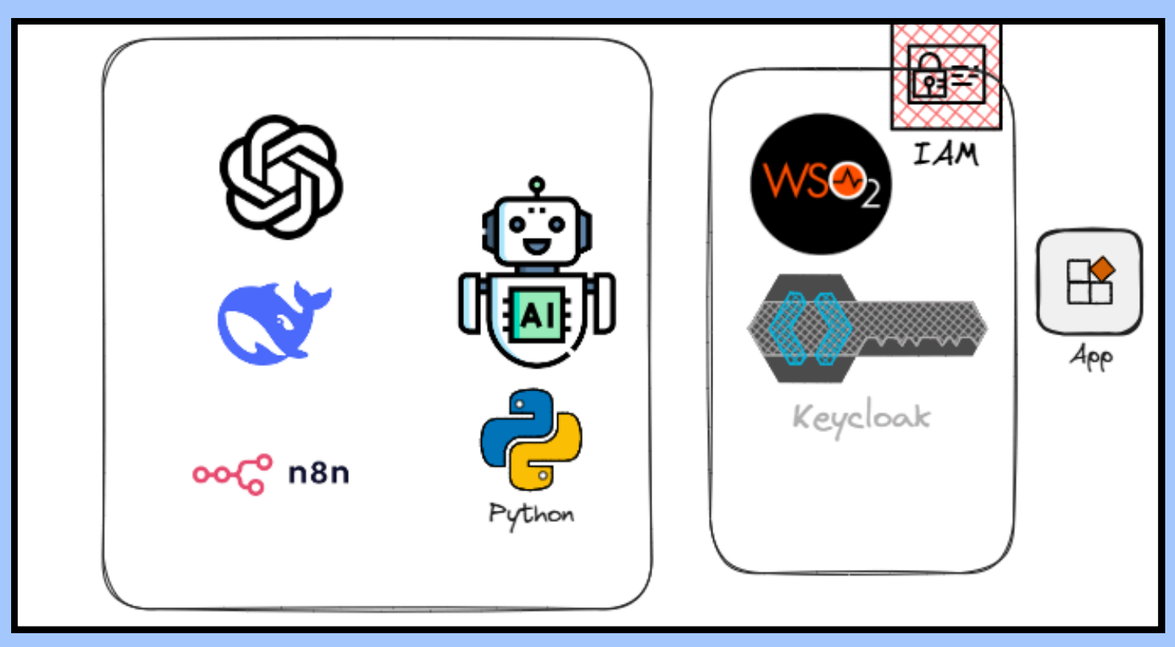
2-Técnica que consiste en un **modelo doble factor de autenticación basado en smart contracts desplegados en blockchain** que no haga uso de proveedores de identidad de terceros, con un enfoque en la privacidad y la seguridad.

3-diseño y ejecución de pruebas de tipo read team a los sistemas de IAM insertos en aplicaciones web.

4-Concientización en el uso de la **identidad autosoberana (SSI)**.

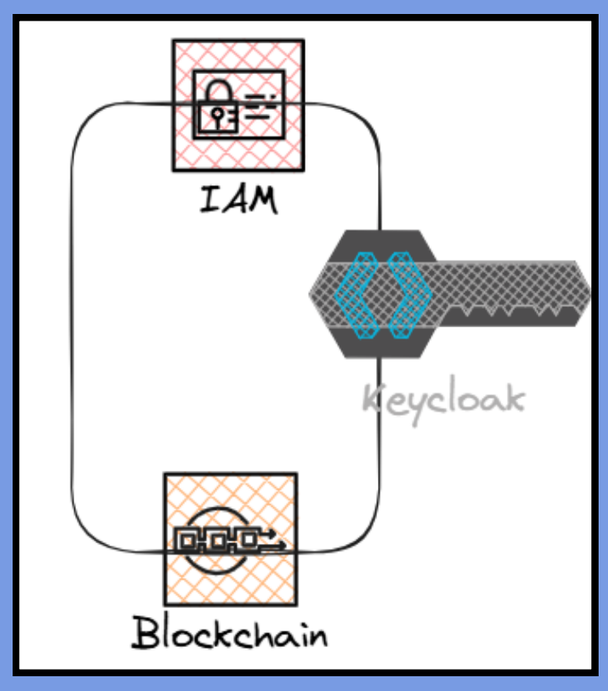
AGENTES DE IAM

Diseñar agentes inteligentes de IAM en Python, realizar entrenamientos y analizar como se comportan. Se pretende desarrollar e integrar los agentes inteligentes en los gestores de gestión de identidad y acceso de código abierto Keycloak y WSO2.

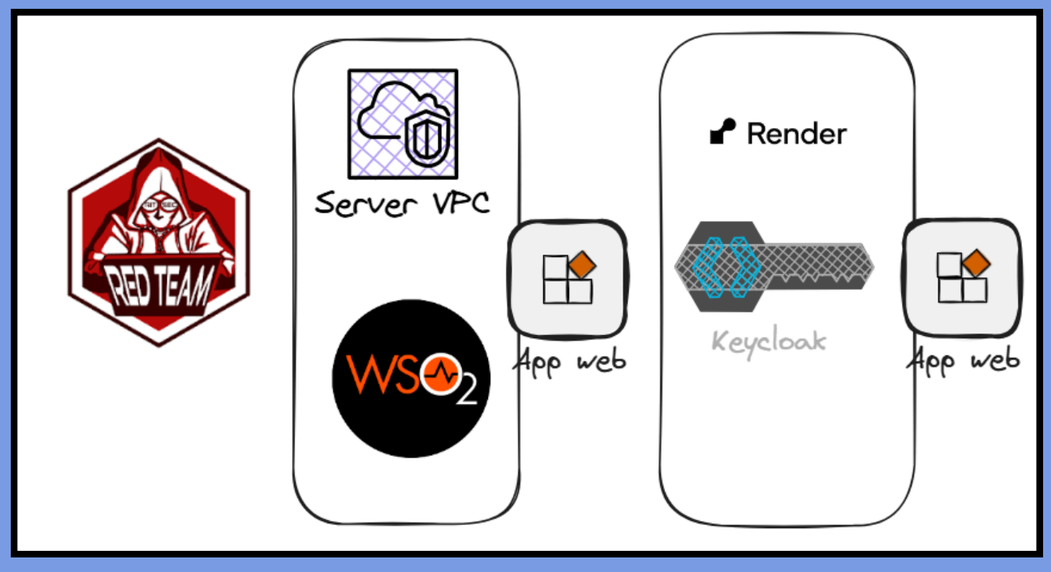


IAM EN BLOCKCHAIN

Modelo doble factor de autenticación basado en smart contracts desplegados en blockchain



ARQUITECTURA EN AMBIENTES WEB 2



Pruebas de tipo read team a los sistemas de IAM insertos en aplicaciones web.

RESULTADOS ESPERADOS

Generar, al menos, un agente de inteligencia artificial que se pueda integrar a los gestores de identidad Keycloak y WSO2 Identity Server

Medir y ponderar acerca del rendimiento y niveles de seguridad del agente generado, con el objetivo de definir el grado de protección que ofrece a la identidad del usuario y cómo influye en la experiencia de usuario.

Concluir si el uso de tecnologías descentralizadas Web3 mejoran los niveles de seguridad en aplicaciones web respecto a tecnología vinculadas a las Web2