**Elevator Speech**

La Cuarta Revolución Industrial, conocida como Industria 4.0, está transformando radicalmente el entorno industrial a través de la digitalización y la integración de tecnologías avanzadas como IoT, inteligencia artificial y automatización. Sin embargo enfrentan desafíos a la hora de proteger datos críticos.

Con el crecimiento de la Industria 4.0, enfrentamos una complejidad creciente en los sistemas, lo que dificulta garantizar la seguridad y adaptabilidad. La necesidad de detectar de manera temprana las vulnerabilidades del sistema es crucial para evitar fallos operativos y proteger datos críticos.

Aunque las medidas tradicionales como cifrado, autenticación, capacitación en seguridad y redundancia son fundamentales, presentan limitaciones significativas: el cifrado es inútil si las claves son comprometidas, la autenticación puede fallar ante ataques como phishing, los errores humanos siguen siendo el eslabón más débil y la redundancia mal diseñada puede ser un blanco fácil para atacantes. Por ello, es esencial complementarlas con herramientas avanzadas como la detección de anomalías en tiempo real, capaces de identificar y responder a comportamientos sospechosos antes de que se conviertan en amenazas críticas.

Un módulo de detección de anomalías es crucial en sistemas industriales, ya que permite una supervisión constante para identificar desviaciones en el comportamiento normal y responder de forma temprana, minimizando riesgos y costos. Sin embargo, enfrenta desafíos clave como procesar grandes volúmenes de datos en tiempo real, garantizar la precisión algorítmica para distinguir entre variaciones normales y anomalías reales, y manejar el balance entre falsos positivos, que generan alertas innecesarias, y falsos negativos, que podrían pasar desapercibidos y causar fallos críticos. Estos aspectos hacen indispensable un diseño robusto y adaptativo.

En los sistemas industriales, la detección de anomalías emplea métodos como Isolation Forest, Z-Score, DBSCAN y Autoencoders. Cada uno de ellos aporta beneficios únicos dependiendo de las características de los datos. Por ejemplo, Isolation Forest es eficiente en datos de gran volumen, mientras que los Autoencoders destacan en contextos de alta dimensionalidad. Z-Score brilla cuando los datos siguen una distribución normal y el fuerte de DBSCAN se encuentra en los datasets densos.

El desafío radica en diseñar un módulo que pueda seleccionar automáticamente el mejor algoritmo según las características de los datos, garantizando precisión en la detección de anomalías en tiempo real. Este problema es especialmente relevante en entornos industriales simulados, donde las variables cambian constantemente.

Para abordar este desafío, se utilizó como objeto de estudio un entorno industrial simulado compuesto por:

1. Sensores

2. Microcontroladores STM32

3. PLC basado en OpenPLC

Para validar la propuesta, se comparó el rendimiento de algoritmos implementados en Python frente a herramientas como Knime. Los resultados demuestran que el módulo mejora significativamente la seguridad, reduce falsos positivos y negativos, y asegura una respuesta rápida ante posibles anomalías.

Impacto Potencial:

Este módulo no solo aumenta la resiliencia de los sistemas industriales, sino que también establece un nuevo estándar en la gestión de la seguridad, fortaleciendo la transformación digital en la Industria 4.0.

En conclusión, la detección de anomalías en tiempo real es un componente clave para la seguridad de la Industria 4.0. Este módulo innovador no solo optimiza los procesos, sino que también asegura la continuidad operativa, contribuyendo a una industria más segura y eficiente."