

WATCHNET: PLATAFORMA DE MONITOREO DE RED CON NOTIFICACIONES PREDICTIVAS DE ESTADO Y VULNERABILIDADES

PROBLEMA

En un mundo cada vez más interconectado, las redes de datos desempeñan un papel fundamental en el funcionamiento eficiente de empresas, instituciones y usuarios en general. La estabilidad, eficiencia y calidad de una red se han convertido en factores críticos que influyen directamente en la experiencia de los usuarios y en la optimización de los recursos de conectividad.

OBJETIVO GENERAL

Desarrollar una plataforma de monitoreo de red basada en técnicas de Machine Learning que permita la predicción de posibles problemas de vulnerabilidades y rendimiento en la red del centro de investigación CTI, evitando posibles ataques y mejorando la calidad de servicio ofrecida a sus usuarios.

PROPUESTA

La plataforma de monitoreo de red que se plantea busca ir más allá de la detección y solución de problemas concurrentes. Con un enfoque proactivo se pretende anticipar posibles vulnerabilidades, identificar el estado de la red y evaluar su rendimiento, permitiendo a los administradores y el área de TI tomar decisiones informadas y realizar ajustes preventivos para garantizar una red estable, eficiente y segura. Analizando redes cableadas y redes inalámbricas cada vez más utilizadas en entornos empresariales y domésticos. La optimización de la red inalámbrica se ha convertido en un desafío importante debido a la creciente demanda de dispositivos móviles y la necesidad de una conectividad de calidad.

Así mismo, se implementarán algoritmos de aprendizaje automático para entrenar un modelo que permita pronosticar posibles vulnerabilidades y problemas de rendimiento. Posteriormente, se enviarán notificaciones a través de la plataforma de monitoreo para informar sobre dichas incidencias.

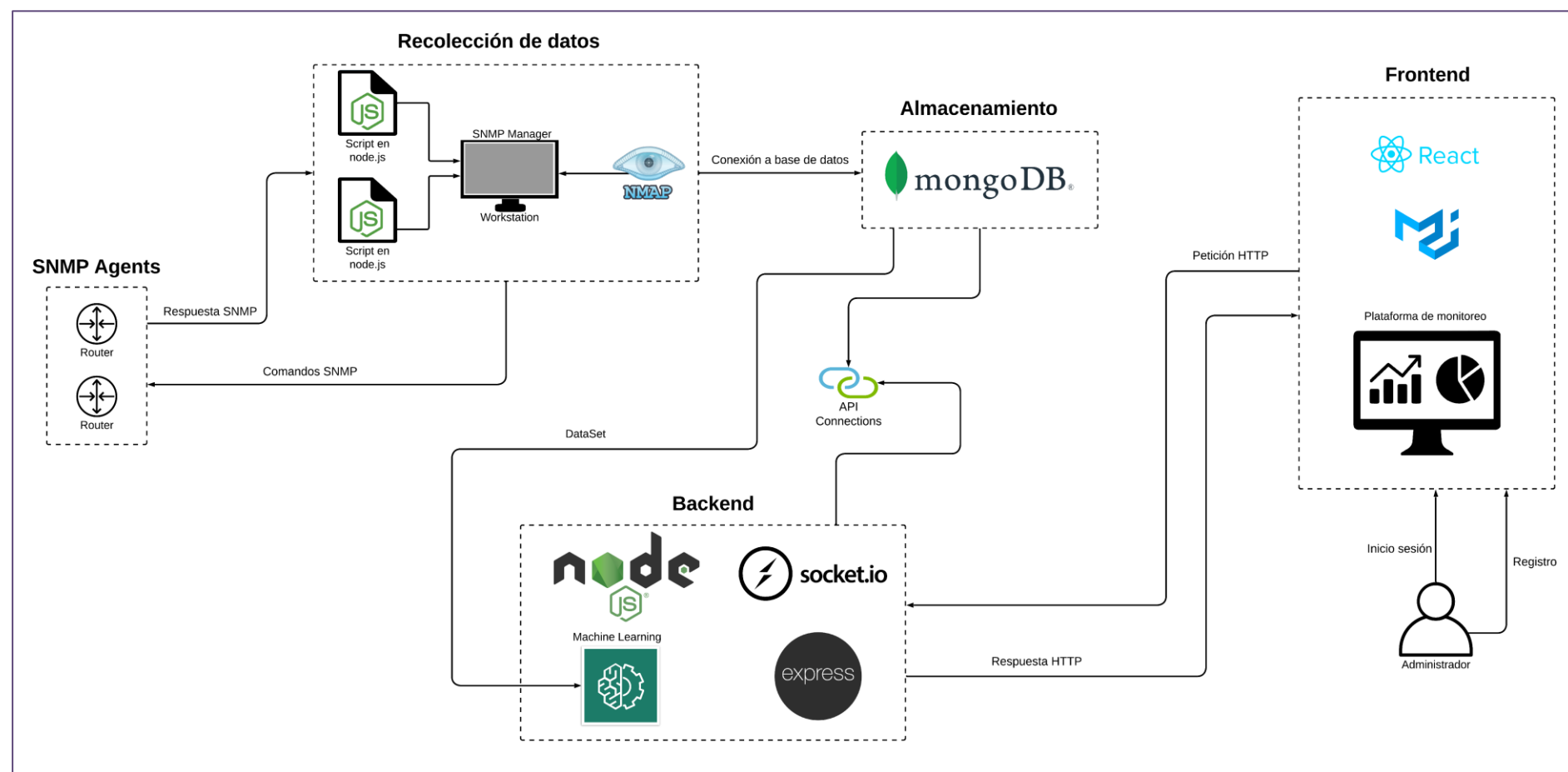


Figura 2. Diagrama del sistema propuesto.

RESULTADOS



Figura 3. Resultados obtenidos a partir de los datos registrados por la plataforma web

En la plataforma web WatchNet, se puede observar información sobre la red y los dispositivos conectados a ella cómo se evidencia en la pantalla de Dispositivos conectados, además de obtener información de los puertos expuestos de dichos dispositivos. Finalmente, también se puede medir las métricas de desempeño de la red analizada que se encuentran en el panel principal.

CONCLUSIONES

La incorporación de técnicas de Machine Learning, como el modelo ARIMA, ha demostrado ser efectiva al momento de realizar predicciones en el rendimiento de la red. Esto resalta el potencial de la plataforma implementada para mejorar la seguridad y el rendimiento de la infraestructura de red analizada.

La implementación de notificaciones sobre los puertos abiertos expuestos permite una respuesta rápida y proactiva ante posibles vulnerabilidades y riesgos de seguridad. Esto ayuda a fortalecer la postura de seguridad del centro de investigación CTI, evitando posibles ataques y protegiendo la integridad de la red y los datos.

La administración de la plataforma de monitoreo de redes se concibió con la premisa de incorporar diversas alternativas de monitoreo y ajustarse a las necesidades específicas de diversos tipos de routers, con el objetivo fundamental de lograr una perfecta integración en cualquier arquitectura, sin importar la naturaleza del router disponible. Esto se llevó a cabo con el propósito de asegurar su versatilidad y facilidad de incorporación y manipulación.