Sistemas autónomos en servidores: del monitoreo reactivo a la prevención predictiva

Автономные системы на серверах: от реактивного мониторинга до прогнозирования и предотвращения угроз.

Bernardo Román Hernandez, Gonzalo Tobon Solis, María del Carmen Santiago Díaz, Ana Claudia Zenteno Vázquez, Gustavo Trinidad Rubín Linares

Facultad de Ciencias de la Computación, Benemérita Universidad Autónoma de Puebla, Av. San Claudio, s/n. 72570 Puebla, Puebla

{bernardo.roman, gonzalo.tobon}@alumno.buap.mx, {marycarmen.santiago, ana.zenteno, gustavo.rubin}@correo.buap.mx

Resumen: La gestión de infraestructuras de TI enfrenta una complejidad creciente debido a la nube, microservicios, IoT y Big Data. Los sistemas distribuidos a gran escala exigen alta disponibilidad, superando los métodos manuales. Este informe explora la transición necesaria del monitoreo reactivo tradicional a la prevención predictiva, impulsada por los conceptos de Computación Autónoma y las tecnologías de Inteligencia Artificial para Operaciones de TI (AIOps). Se analizan los principios de auto-gestión ("self*"), el ciclo MAPE-K, la evolución del monitoreo, las tecnologías clave de AIOps (especialmente Machine Learning), sus beneficios y desafíos, y su aplicación en arquitecturas modernas como microservicios, ejemplificado por el framework FIRM. El objetivo es proporcionar una comprensión fundamentada de esta evolución hacia una gestión de servidores más inteligente y resiliente.

Аннотация: Управление ИТ-инфраструктурой сталкивается с растущей сложностью из-за облачных технологий, микросервисов, Интернета вещей и больших данных. Крупномасштабные распределенные системы требуют высокой доступности, превосходящей ручные методы. В этом отчете рассматривается необходимый переход от традиционного реактивного мониторинга к предиктивному предотвращению, основанный на концепциях автономных вычислений и технологиях искусственного интеллекта для ИТ-операций (AIOps). В нем анализируются принципы самоуправления, цикл MAPE-K, эволюция мониторинга, ключевые технологии AIOps (особенно машинное обучение), их преимущества и проблемы, а также их применение в современных архитектурах, таких как микросервисы, на примере фреймворка FIRM. Цель состоит в том, чтобы обеспечить обоснованное понимание этой эволюции в сторону более интеллектуального и отказоустойчивого управления серверами.

Frases y palabras clave: Sistemas Autónomos, AIOps, Monitoreo Predictivo, Gestión de Servidores, Computación Autónoma, Machine Learning, Microservicios, Prevención de Fallos.

Ключевые слова и фразы: Архитектура программного обеспечения, Сервис-ориентированная архитектура, Электронное обучение,

_____

1 Introducción

La gestión de infraestructuras de TI modernas es cada vez más compleja debido a las nuevas tecnologías, arquitecturas o paradigmas en los últimos años, por ejemplo, la nube híbrida/multi-nube, microservicios, IoT y Big Data. Los sistemas críticos son aquellos sistemas cuya falla, interrupción o un mal funcionamiento puede generar graves consecuencias tanto en lo económico, social y operativo, por lo tanto, se requiere una alta fiabilidad, pero la escala y dinamismo desafían los métodos manuales, que resultan insuficientes. Actualmente, se encuentran en desarrollo los siguientes enfoques que buscan dar solución a estos desafíos:

- Sistemas Autónomos: Inspirados en sistemas biológicos, buscan autogestionarse (configuración, optimización, reparación, protección - "self*") según objetivos de alto nivel, con mínima intervención humana.
- Monitoreo Predictivo: Enfoque proactivo que usa modelos estadísticos y ML para analizar datos y predecir incidentes (fallos, cuellos de botella) antes de que ocurran.

Antes de estos enfoques lo más común era la gestión tradicional que se basaba en el monitoreo reactivo, detectando problemas después de ocurridos (umbrales estáticos), lo que causa downtime (tiempo en que un sistema, servicio o equipo no está disponible) y respuestas lentas. Es por ello por lo que el monitoreo proactivo introdujo automatización y correlación (ITSM), permitiendo predecir algunos fallos basados en tendencias, pero aún limitado ante la complejidad actual. La prevención predictiva es el salto cualitativo: usa IA/ML para predecir con precisión, prescribir e incluso ejecutar acciones correctivas para evitar fallos. Comprender esta transición es muy importante. Por ello, este artículo explora los sistemas autónomos, AIOps, técnicas de ML, beneficios y desafíos.

2 La Evolución del Monitoreo de Servidores

El monitoreo de servidores ha recorrido un camino significativo, desde simples alertas manuales hasta plataformas inteligentes capaces de predecir y resolver problemas antes de que afecten a los usuarios. Esta evolución refleja el avance hacia sistemas más autónomos, resilientes y eficientes, impulsados por la necesidad de manejar entornos cada vez más dinámicos y distribuidos.

2.1 Monitoreo Reactivo Tradicional

En esta etapa, los sistemas se basan en la vigilancia constante de métricas clave como lo son: CPU, memoria, disco, red, etcétera, y mediante la comparación con umbrales estáticos definidos por el administrador del sistema se genera una alerta cuando dicho umbral es superado, por lo tanto, los problemas se están detectando después de ocurridos.

A continuación, se presenta una descripción resumida del monitoreo reactivo tradicional y sus limitaciones más relevantes:

Tabla 1. Comparativa de Paradigmas de Monitoreo de Servidores.

Aspecto	Descripción
Métricas monitoreadas	CPU, Memoria, Disco, Red, etc.
Método de Alerta	Generación de alertas cuando se superan umbrales estáticos predefinidos.
Herramientas típicas	- Nagios: Monitorización de redes, código abierto. - Zabbix: Monitoreo gráfico y alertas automatizadas. - Munin: Visualización de métricas históricas.
Limitaciones	1. MTTD (Mean Time to Detect) y MTTR (Mean Time to Repair) elevados. 2. Alta tasa de falsas alarmas. 3. Imposibilidad de detectar patrones ocultos. 4. Reacción tardía, prolongando el downtime.

2.2 Hacia el Monitoreo Proactivo

Este enfoque representa un paso intermedio hacia la autonomía. Aquí es donde se incorporan reglas más sofisticadas y la incorporación de automatización a las respuestas básicas. Ejemplos de esto son scripts, reinicios, limpieza de cachés, e integración con herramientas de gestión de servicios TI como ITSM (IT Service Management) entre otras acciones, lo cual nos permite tener una reacción más ágil, pero sigue siendo limitado ante comportamientos imprevistos.

Algunas de las herramientas tecnológicas claves para este enfoque son las siguientes:

- Splunk, ELK Stack (Elasticsearch, Logstash, Kibana) usados para correlación de eventos y análisis de logs.
- Prometheus con Alertmanager, el cual es útil para métricas de sistemas distribuidos en tiempo real.

A comparación del monitoreo reactivo tradicional tenemos las siguientes mejoras:

- Se correlacionan múltiples métricas o eventos para comprender mejor un incidente.
- Se realizan predicciones simples basadas en tendencias lineales o umbrales dinámicos.

- Se integran con flujos de trabajo automáticos, por ejemplo, para reiniciar servicios al detectar ciertos logs.

Aunque este enfoque representa un gran avance todavía tiene limitaciones persistentes como:

- No adaptativo: depende de reglas predefinidas, que pueden volverse obsoletas ante nuevas arquitecturas (e.g., microservicios o serverless).
- Es incapaz de aprender de experiencias pasadas o evolucionar con el entorno.
- Sensible a "alert fatigue" (fatiga de alertas) por la sobrecarga de notificaciones sin contexto.

2.3 Prevención Predictiva: El Salto Cualitativo

Con la llegada de **AIOps (Artificial Intelligence for IT Operations)** el cual se explicará más adelante, la prevención predictiva representa una nueva frontera: no solo se busca detectar fallos antes de que ocurran, sino que también sugiere soluciones (prescripción) y, en algunos casos, las ejecuta automáticamente (autoremediación).

En este enfoque, gracias a la tendencia y al desarrollo de áreas avanzadas como la inteligencia artificial y el análisis de datos, se utilizan tecnologías clave como las siguientes:

- Machine Learning supervisado y no supervisado para detección de anomalías, así como la regresión y clasificación de incidentes.
- Deep Learning para análisis de logs y patrones de uso en tiempo real.
- Plataformas como Moogsoft, Dynatrace, Datadog, y Splunk ITSI, que combinan AIOps con automatización.

Gracias a estas técnicas tenemos capacidades avanzadas para el monitoreo:

- Detección de *anomalías contextualizadas* (e.g., una subida de CPU puede no ser anómala si ocurre durante un despliegue planificado).
- Predicción de eventos futuros como la saturación de recursos o la degradación de servicios.
- Generación de *insights prescriptivos* (recomendaciones para evitar o mitigar incidentes).
- Automatización de respuestas usando plataformas orquestadas como Ansible, Chef o Kubernetes Operators.

Tabla 2. Comparativa de Paradigmas de Monitoreo de Servidores.

Característica	Monitoreo Reactivo	Monitoreo Proactivo	Prevención Predictiva (AIOps)
Timing	Después del incidente	Antes del impacto (tendencias)	Antes del incidente (predicción)

Enfoque	Respuesta a fallos	Patrones, automatización	Prevención, optimización
Uso de Datos	Umbrales estáticos	Tiempo real, correlación	Big Data (histórico, tiempo real)
Técnicas	Reglas básicas	Correlación, scripts	ML (Supervisado, No Sup., RL), IA
Objetivo	Resolver, minimizar downtime	Reducir downtime, eficiencia	Prevenir downtime, optimizar, autoreparar
Herramientas	Nagios, Zabbix	ServiceNow, Splunk	Plataformas AIOps, ML

Esta tabla refleja la creciente complejidad de la infraestructura y una mayor dependencia de datos operativos de calidad y volumen. La falta de datos de calidad es una barrera para AIOps.

3 Computación Autónoma y Sistemas Autogestionados

La prevención predictiva se basa en los principios de la Computación Autónoma conocida como AC, esta visión es propuesta por IBM en el año de 2001 para crear sistemas capaces de autogestionarse con mínima intervención humana, esta se basa en sistemas biológicos como lo es el sistema nervioso. La importancia de estos sistemas es muy significativa en áreas de TI, donde las acciones que se requieren son muy complejas y dinámicas y donde la escalabilidad y la resiliencia son críticas.

3.1 Conceptos Fundamentales

La Computación Autónoma se centra en los sistemas con propiedades **"self*"** autonómicas), que permiten adaptarse a cambios imprevistos. Esta visión fue desarrollada por Jeffrey O. Kephart y David M. Chess la cual se menciona en el artículo The Vision of Autonomic Computing y por IBM en su manifiesto sobre AC enfatizando la analogía existente entre los sistemas biológicos autorregulados. Estas cuatro capacidades clave son:

- Auto-Configuración(Self-configuring): Ajuste automático de parámetros ante nuevos componentes o entornos (ej.: escalado en la nube).
- Auto-Optimización(Self-optimizing): Mejora continua de rendimiento mediante análisis de métricas (ej.: balanceo de cargas con ML).
- Auto-Reparación(Self-healimg):: Detección y mitigación de fallos (ej.: reinicio de contenedores en Kubernetes).
- Auto-Protección(Self-protecting):: Identificación proactiva de amenazas (ej.: respuesta a ataques DDoS).

3.2 El Ciclo MAPE-K

Propuesto por IBM en 2003 como parte de su arquitectura de referencia para sistemas autónomos es el estándar para implementar estos sistemas [2]. En donde cada fase que se muestra a continuación se potencia con IA/ML en contextos modernos:

- Monitor: Recopilación de datos en tiempo real (métricas, logs, trazas).
  - o Herramientas: Prometheus, Open Telemetry.
- Analyze: Identificación de patrones/anomalías mediante ML (AIOps).
  - o Técnicas: Redes neuronales para detección de outliers (LSTM).
- Plan: Generación de acciones (ej.: escalar recursos).
  - o Ejemplo: Kubernetes Horizontal Pod Autoscaler.
- Execute: Automatización mediante orquestadores (Ansible, Terraform).
- Knowledge: Base de conocimiento unificada (modelos entrenados, políticas).

3.3 Rol en la Gestión Moderna

La Computación Autónoma (AC) y el modelo MAPE-K han sido la base conceptual para el desarrollo de plataformas modernas de gestión TI. Por ejemplo, en el contexto de AIOps, herramientas como Dynatrace aplican modelos de aprendizaje automático (ML) en la fase de análisis para correlacionar eventos y detectar problemas con mayor precisión. En cuanto a sistemas de auto-reparación, plataformas como Moogsoft utilizan procesamiento de lenguaje natural (NLP) para interpretar registros (logs) y diagnosticar fallos de forma automática. En el ámbito de la nube autónoma, servicios como AWS Auto Scaling emplean reglas predictivas para ajustar dinámicamente los recursos según la demanda del sistema.

Sin embargo, este enfoque también enfrenta desafíos importantes. Uno de los principales es la dependencia de datos históricos de calidad: si los datos no son precisos o están incompletos, los modelos de ML pueden producir resultados erróneos. Además, la autonomía de los sistemas debe estar cuidadosamente alineada con políticas definidas por humanos. No todo debe automatizarse completamente, especialmente en sistemas críticos donde es fundamental establecer límites a la autoreparación o requerir validación humana antes de ejecutar ciertas acciones.

4 AIOps: El Motor de la Prevención Predictiva

4.1 Objetivos Clave

AIOps (Artificial Intelligence for IT Operations) es un enfoque que combina diferentes tecnologías y áreas como la inteligencia artificial (IA), aprendizaje automático (ML) y análisis de big data para automatizar y optimizar las operaciones de TI. Su objetivo principal es el anticipar y prevenir fallos en sistemas antes de que ocurran, esto permite una gestión proactiva en lugar de reactiva y hace que se mejore la disponibilidad y eficiencia de los sistemas. Esto se logra mediante el análisis en

tiempo real de grandes cantidades de datos provenientes de registros, métricas, y eventos, para así poder identificar patrones y anomalías que podrían significar grandes problemas.

En un estudio que lleva como nombre: *"Agentic AI in Predictive AIOps: "Enhancing IT Autonomy and Performance"* se menciona cómo AIOps puede mejorar la autonomía y el rendimiento de los sistemas de TI al integrar inteligencia artificial y así predecir, identificar y resolver problemas de manera proactiva, minimizando el tiempo de inactividad y mejorando por mucho la eficiencia operativa.

4.2 Tecnologías Habilitadoras

Como se mencionaba, una implementación efectiva de AIOps se basa en varias tecnologías clave como:

- **Aprendizaje Automático (Machine Learning)**: Para facilitar el análisis de datos para identificar patrones y predecir posibles fallos.
- **Procesamiento del Lenguaje Natural (NLP)**: Nos ayuda en la interpretación de datos no estructurados, como registros de texto y tickets de soporte.
- **Big Data**: Nos permite la recopilación y el almacenamiento de grandes volúmenes de datos generados por las infraestructuras de TI.

Automatización: Permite la ejecución de acciones correctivas sin intervención humana, mejorando la eficiencia operativa.

4.3 Beneficios

Como se ha estado mencionando, uno de los beneficios más importantes al implementar AIOps es la prevención proactiva de fallos, ya que estas tecnologías permiten anticipar los posibles problemas antes de que estos ocurran y gracias a esto, se logra minimizar la presencia de interrupciones en los servicios, lo que garantiza la funcionalidad operativa.

Ya que, como se está anticipando los posibles problemas también se está reduciendo el tiempo de inactividad. Esto se debe a que las anomalías las cuales son detectadas de forma temprana y, en muchos casos, se resuelven automáticamente, lo que permite mitigar los efectos negativos que pueden surgir durante una interrupción no planeada. Con esto, se observa una optimización de los recursos, ya que el análisis constante del uso y desempeño de la infraestructura permite realizar una asignación más eficiente de los recursos, evitando que se presenten escenarios de sobreutilización o subutilización.

Es importante mencionar que el análisis de datos en tiempo real favorece una mejora en la toma de decisiones, al contar con información oportuna y precisa, sin duda alguna facilita la planeación estratégica y se fortalece la capacidad de respuesta ante eventos críticos que puedan afectar los sistemas. Es por ello por lo que muchas organizaciones han comenzado a implementar AIOps como un recurso esencial en su transición hacia entornos de TI más inteligentes.

5 Implementación Práctica y Arquitecturas

Una implementación de AIOps no es trivial, ya que involucra tanto decisiones técnicas como organizacionales, y se requiere una planificación muy detallada que contemple tanto las capacidades actuales como las metas futuras de la organización. A continuación, se presentan los principales elementos a considerar en su implementación.

5.1 Consideraciones Arquitectónicas

Para que una organización adopte la integración de AIOps se quiere una estructura flexible y escalable que sea capaz de manejar grandes volúmenes de datos en tiempo real, por ello, es fundamental contar con una arquitectura orientada a eventos, y con esto queremos decir que los sistemas puedan generar, recolectar y transmitir información de forma continua. Donde dicha información proviene de diversas fuentes como lo son logs, métricas de rendimiento, trazas, y tickets de soporte. También, una de las principales consideraciones es que los sistemas de monitoreo existentes en la organización estén integrados de manera fluida ya que esto nos garantiza que los datos fluyan sin interrupciones ni incompatibilidades.

El enfoque de la arquitectura AIOps está diseñada en capas, por lo tanto, existe una separación entre la capa de recolección de datos, la capa de procesamiento (normalización, enriquecimiento y correlación), y finalmente, la capa de inferencia y automatización. Esta separación no solo facilita el mantenimiento, sino que también permite la actualización modular conforme evolucionen las tecnologías involucradas. Es por ello que muchos esquemas arquitectónicos actuales proponen el uso de microservicios, contenedores y pipelines de datos en tiempo real y habilitados a través de herramientas como Apache Kafka, Prometheus, Grafana, y motores de análisis como Elasticsearch o Splunk.

5.2 Tecnologías de Soporte Contextuales

Una de las tecnologías más relevantes de AIOps es la orquestación basada en contenedores, que permite que las aplicaciones escalen dinámicamente en función de la demanda y reaccionen ante eventos inesperados de forma eficiente. Por ejemplo, el uso de Kubernetes se ha convertido en un estándar por su capacidad de manejar cargas de trabajo distribuidas y autoescalables.

Otra tecnología clave es la integración de herramientas de ITSM (Gestión de Servicios de TI) la cual se ha mencionado anteriormente, y como ejemplos están ServiceNow o BMC Helix, que proporcionan contexto adicional a los eventos y ayudan a cerrar el ciclo completo de observación, decisión y acción. También, se puede destacar el uso de bases de datos no relacionales como MongoDB y Cassandra, ideales para el almacenamiento rápido y flexible de información heterogénea y de gran volumen.

Por último, se requiere una infraestructura de red que soporte una alta disponibilidad y baja latencia, dado que la eficiencia de AIOps depende en gran medida de la velocidad con la que los datos se transmiten y procesan para generar conocimientos relevantes.

5.3 Estudio de Caso - Gestión Inteligente de Recursos con FIRM

Se analizó la implementación del modelo FIRM (Flexible Infrastructure Resource Management), el cual fue adoptado por una organización de servicios financieros con el objetivo de gestionar de

manera más eficiente sus recursos tecnológicos [5]. Este modelo se conforma por diferentes herramientas de monitoreo de infraestructura, como modelos entrenados de machine learning para la predicción de carga de trabajo, y reglas automatizadas para la asignación de los recursos computacionales.

Para su implementación se requirió establecer una arquitectura distribuida basada en microservicios y análisis en tiempo real, utilizando la plataforma de código abierto Apache Flink para el procesamiento de eventos y flujos de da datos en tiempo real y TensorFlow que claramente esta es una librería muy usada para construir y entrenar modelos para la predicción con machine learning y Deep learning. Y con la integración con el sistema de tickets con la cual se documentan y gestionan los problemas reportados o detectados automáticamente, permitió la correlación directa entre eventos detectados y las acciones correctivas, reduciendo así el tiempo medio de resolución en que se tarda en resolver un incidente desde que se detecta hasta que se soluciona (MTTR) en un 35 %, donde una MTTR baja significa alta eficiencia operativa.

Según los resultados del artículo con el uso del modelo FIRM, se observaron mejoras en la eficiencia operativa, en la disponibilidad del sistema y una gran reducción significativa en los costos de operación. Este caso que exponemos evidencia cómo una correcta aplicación de AIOps puede convertirse en una herramienta estratégica para alcanzar una gestión inteligente y sostenible de recursos tecnológicos.

6 Desafíos y Direcciones Futuras

6.1 Obstáculos en la Implementación

Para la implementación de AIOps se enfrentan diversos obstáculos que deben ser considerados para lograr una adopción efectiva. Uno de los principales retos es cuando se requieren entrenar modelos de inteligencia artificial, ya que esto necesita la calidad, disponibilidad y diversidad de los datos, estos son elementos esenciales para alimentar dichos modelos y así obtener resultados confiables de las predicciones. A esto se suma la complejidad algorítmica y de los sistemas que soportan estas soluciones, lo cual implica desafíos técnicos significativos. Además, uno de los obstáculos es la falta de personal especializado en áreas como ciencia de datos, ingeniería de datos e inteligencia artificial, lo que dificulta la formación de equipos capaces de diseñar, desplegar y mantener estos sistemas. Otro factor muy limitante y que es necesario mencionarlo es el alto costo computacional, pues especialmente en el uso de modelos de lenguaje de gran tamaño (LLMs), cuyo entrenamiento y ejecución requieren recursos intensivos que en muchas ocasiones están al alcance de las organizaciones. De igual manera, otro de los obstáculos, es la preocupación sobre la confianza, la interpretabilidad y los riesgos asociados al uso de IA, como lo puede ser el sobreajuste o el ruido que pueden tener los datos afectan la precisión de los resultados y si son usados así pueden llevar a decisiones erróneas.

6.2 El Futuro de la Gestión Autónoma

El futuro de la gestión autónoma en entornos de TI se vislumbra como un escenario de colaboración estrecha entre humanos e inteligencia artificial, esto porque se espera una mayor

autonomía a través de la adopción de inteligencia agentiva (Agentic AI), en donde agentes inteligentes actuarán de forma coordinada y de manera completa para gestionar de manera integral los incidentes que puedan surgir. Asimismo, se espera una integración profunda de modelos de lenguaje (LLMs) y aunque podríamos decir que se encuentran en auge aún hay grandes desafíos técnicos y limites en generalización e integración. Estos modelos se espera que sean más poderosos y confiables y asi poder realizar análisis semánticos, llevar a cabo procesos de análisis de causa raíz (RCA), generar soluciones y facilitar la operación mediante herramientas como ChatOps. Será necesario superar importantes barreras relacionadas con los costos y la confiabilidad de estos modelos. Otro aspecto relevante será el aumento de las capacidades humanas mediante la colaboración con la IA, permitiendo que esta se encargue de las tareas rutinarias y de gran escala, mientras que los profesionales humanos aportarán su juicio crítico y estratégico, ya que lo que se busca es que sea una herramienta útil para las personas y organizaciones. Este enfoque apunta a potenciar la eficiencia sin perder de vista el valor del conocimiento humano. Por último, se prevé que los sistemas de AIOps evolucionen hacia un modelo de optimización continua y autoaprendizaje, donde los algoritmos mejoren sus propios procesos y estrategias con base en la experiencia operativa acumulada.

7 Conclusiones y trabajos futuros

La transición del monitoreo reactivo a la prevención predictiva representa un cambio fundamental en la gestión de infraestructuras TI. En un entorno caracterizado por su creciente complejidad y dinamismo, como el que imponen la nube, los microservicios, IoT y Big Data, los métodos tradicionales resultan insuficientes. La adopción de enfoques basados en Computación Autónoma y AIOps permite a los sistemas no solo detectar y responder a fallos, sino anticiparse a ellos y actuar de forma autónoma. Esto no solo mejora la disponibilidad y el rendimiento, sino que también reduce significativamente el tiempo de inactividad y la carga operativa del personal técnico. Sin embargo, este avance también impone nuevos desafíos, como la necesidad de datos de alta calidad, la interpretación contextual de anomalías y la integración efectiva de herramientas inteligentes. En suma, el futuro de la gestión de servidores se perfila como un entorno auto-adaptativo y resiliente, donde la inteligencia artificial juega un papel clave para alcanzar una verdadera autonomía operativa.

Referencias

[1] V. Funda and E. Francke, “Benefits and challenges of AIOPS adoption and usage in HEIs in developing countries”, SAJHE, vol. 38, no. 6, pp. 56-78, Nov. 2024.

[2] J. O. Kephart and D. M. Chess, "The vision of autonomic computing," in Computer, vol. 36, no. 1, pp. 41-50, Jan. 2003, doi: 10.1109/MC.2003.1160055.

[3] A. M. Manasrah, T. Khdour, and R. Freehat, "DGA-based botnets detection using DNS traffic mining," Journal of King Saud University - Computer and Information Sciences, vol. 34, no. 5, pp. 2045-2061, 2022, doi: 10.1016/j.jksuci.2022.03.001.

[4] P. Kruchten, S. Fraser, and F. Coallier, Eds., *Agile Processes in Software Engineering and Extreme Programming: 20th International Conference, XP 2019, Montréal, QC, Canada, May 21–25, 2019, Proceedings*. Cham: Springer Cham, 2019.

[5] H. Qiu, S. S. Banerjee, S. Jha, Z. T. Kalbarczyk y R. K. Iyer, "FIRM: An Intelligent FineGrained Resource Management Framework for SLO-Oriented Microservices," en Proceedings of the 14th USENIX Symposium on Operating Systems Design and Implementation (OSDI 20), USENIX Association, 2020, pp. 805–825. DOI: 10.48550/arXiv.2008.08509

[6] Guo, Z., Chen, H., & Wang, Y. (2021). AIOps: Real-World Challenges and Research Innovations. Proceedings of the 2021 IEEE International Conference on Cloud Computing (CLOUD). https://doi.org/10.1109/CLOUD53861.2021.00027

[7] Ghosh, S., & Sharma, D. (2021). Predictive Analytics in IT Operations Using Machine Learning Techniques: A Survey. Journal of Network and Computer Applications, 177, 102930.

[8] Sivaraman, V., & Khosla, R. (2020). Autonomous Computing Systems: Challenges and Design Considerations. ACM Computing Surveys, 53(6), 1–31.

[9] Ahmed, S., Singh, M., Doherty, B., Ramlan, E., Harkin, K., & Coyle, D. (2023). AI for Information Tecchnology Operation (AIOps): A Review of IT Incident Risk Prediction. In 2022 9th International Conference on Soft Computing and Machine Intelligence, ISCMI 2022 (pp. 253-257). (2022 9th International Conference on Soft Computing & Machine Intelligence (ISCMI)). IEEE. Advance online publication. https://doi.org/10.1109/ISCMI56532.2022.10068482

[10] Zhang, Y., Bi, J., & Xu, X. (2020). AIOps: Real-world challenges and research innovations. Frontiers of Computer Science, 14, 1–16. https://web.eecs.umich.edu/~ryanph/paper/aiops-icse19-briefing.pdf