# Tema: Vulcloud Scalable and Hybrid Vulnerability Detection in Cloud Computing

## Síntesis:

En la actualidad las vulnerabilidades de seguridad dan lugar a las famosas brechas de seguridad o violaciones de la política de seguridad del sistema, esto provoca fugas de información y muchas veces pérdidas económicas. Ya se nos han presentado métodos de detección como el análisis estático, el análisis dinámico y las pruebas de fuzzing

Vulcloud es una arquitectura basada en computación en la nube diseñada para detectar vulnerabilidades en el software. Está diseñado es para hacer frente a los siguientes desafíos:

* detección de falsos positivos
* falsos negativos
* cobertura del código fuente
* excepciones de ejecución.

Vulcloud se encarga de analizar estéticamente los objetos e informa sobre los posibles elementos vulnerables, también en el apartado se nos muestra que los resultados de experimentación muestran que vulcloud puede detectar vulnerabilidades en el software y la computación en la nube resuelve los desafíos de las capacidades de almacenamiento y procesamiento. Para monitorear la ejecución en tiempo real, detectar las excepciones y fallas usando herramientas como Kmemcheck, Kmemleak, Valgrind, etc. El monitoreo en tiempo real es tan importante que, si las causas responsables de la falla no pueden ser identificados, las pruebas de fuzzing no tienen valor.

Con las capacidades de procesamiento y almacenamiento que se cuentan en la computación en la nube, Vulcloud es escalable y es capaz de brindar un servicio privado personalizado cuando sea necesario.

Referencia: Al-Amro H., El-Qawasmeh, E., “Discovering Security Vulnerabilities and Leaks in ASP.NET Websites”, Information Systems Department King Saud University, KSU Riyadh, pp. 329 – 333.