Universitat d'Alacant
Universidad de Alicante

PRÁCTICA: REFLEXIÓN SOBRE MODELADO MATEMÁTICO EN CIBERSEGURIDAD FORENSE

INTRODUCCIÓN AL MODELADO MATEMÁTICO EN CIBERSEGURIDAD FORENSE

En la actualidad, la ciberseguridad es un campo crucial para proteger sistemas informáticos de ataques maliciosos. Uno de los principales retos es la **detección de anomalías en redes de servidores**, donde el tráfico de datos es cada vez más complejo y voluminoso.

El **modelado matemático** juega un papel esencial en la identificación de patrones sospechosos mediante técnicas avanzadas de análisis de datos, que permiten automatizar la detección de amenazas. Sin embargo, este proceso requiere de **un gran poder de cómputo**, que puede limitar la velocidad de respuesta si no se utilizan infraestructuras adecuadas.

Una solución a esta problemática es el uso de la **computación paralela**, que permite analizar múltiples flujos de datos simultáneamente, mejorando el rendimiento y reduciendo los tiempos de detección. En entornos de ciberseguridad, esta técnica puede aplicarse mediante el uso de **aceleradores de hardware** como GPUs (unidades de procesamiento gráfico) y FPGAs (matrices de puertas programables en campo), las cuales permiten ejecutar algoritmos de detección en paralelo con una alta eficiencia.

COMPARACIÓN DE SISTEMAS DE PROCESAMIENTO

Imaginemos dos sistemas distintos utilizados para el análisis de ciberseguridad forense:

1. **Sistema A:** Capacidad de procesamiento de 500 Gigaflops (GFLOPS).
2. **Sistema B:** Capacidad de procesamiento de 10 Teraflops (TFLOPS).

El **Sistema A**, debido a sus limitaciones de cómputo, podría analizar únicamente un subconjunto de tráfico en tiempo real, resultando en tiempos de detección más largos y una posible omisión de ataques críticos.

Por otro lado, el **Sistema B**, gracias a su mayor capacidad de cómputo, podría analizar grandes volúmenes de datos en paralelo, reduciendo los tiempos de respuesta y aumentando la precisión en la detección de amenazas.

DESAFÍOS Y CONSIDERACIONES ÉTICAS

A pesar de las ventajas de la computación paralela, su implementación en el campo de la ciberseguridad plantea desafíos importantes:

- **Éticos:** ¿Cómo garantizar la privacidad de los datos al analizar grandes volúmenes de información?

Ricardo Moreno Rodríguez

- **Técnicos:** ¿Cómo equilibrar el uso de recursos de cómputo para evitar sobrecargas en los sistemas?
- **Operacionales:** ¿Qué costo y complejidad tiene implementar estas soluciones en infraestructuras empresariales o gubernamentales?

OBJETIVO DE LA PRÁCTICA

Los estudiantes analizarán cómo la computación paralela y el uso de aceleradores de hardware pueden mejorar la eficiencia en la detección de anomalías en redes de servidores. Se pretende que, mediante el uso de herramientas de inteligencia artificial, exploren las posibles aplicaciones, beneficios, desafíos y riesgos éticos asociados a este tipo de tecnología en el ámbito de la ciberseguridad.

DESARROLLO DE LA PRÁCTICA

1. **Exploración inicial:**
    - Reflexionar sobre el problema planteado en la introducción.
    - Formular hipótesis sobre la aplicabilidad de la computación paralela en entornos de ciberseguridad.
2. **Uso de inteligencia artificial como herramienta de investigación:**
    - Utilizar herramientas de IA como ChatGPT o Bing AI para investigar:
        - Casos reales de aplicación de la computación paralela en ciberseguridad.
        - Comparación entre sistemas de diferente capacidad de cómputo.
        - Principales desafíos técnicos y éticos asociados.
    - Contrastar la información obtenida con la introducción proporcionada.
3. **Reflexión individual:**
    - Elaborar una reflexión escrita abordando las siguientes cuestiones:
        - **Aplicaciones prácticas:** ¿Cómo podrían usarse estos métodos en empresas o gobiernos para la seguridad de sus redes?
        - **Implicaciones éticas:** ¿Qué riesgos existen en términos de privacidad y vigilancia masiva?
        - **Desafíos técnicos:** ¿Cómo se podrían mejorar estos modelos sin comprometer la eficiencia o la seguridad?
        - **Ventajas e inconvenientes:** ¿Cuáles son los beneficios y posibles problemas de aplicar estas tecnologías?
4. **Discusión en grupo (dependiendo del tiempo disponible):**
    - Si el tiempo lo permite, los estudiantes compartirán sus ideas clave extraídas de su reflexión con el resto de la clase.

   - Se fomentará un debate abierto sobre las ventajas e inconvenientes del uso de la computación paralela en ciberseguridad.
   - Se identificarán puntos en común y discrepancias en sus enfoques.

5. **Entrega del informe:**
   - Subir a Moodle un informe individual con:
     - Resumen de la discusión en clase (si se realiza).
     - Reflexión personal sobre las aportaciones de los compañeros.
     - Propuestas de mejora para la implementación de estos sistemas.

MATERIALES NECESARIOS

- Este documento como referencia.
- Acceso a herramientas de inteligencia artificial (ChatGPT, Bing AI, etc.).
- Moodle para la entrega del informe.

EVALUACIÓN

- **30%** Participación activa en la discusión (si se realiza).
- **40%** Claridad y profundidad en la reflexión individual.
- **30%** Calidad del informe presentado en Moodle.