PROYECTO INTERNO SIN FINANCIAMIENTO PII-DICC-2021-04
Uso de técnicas de minería de datos para la prevención y detección de ataques a bases de datos por inyección de código SQL

En la ciudad de Quito D.M., a los treinta y un días del mes de mayo de dos mil veintitrés, comparecen a la celebración de la presente Acta de Finalización del Proyecto de Investigación Interno sin Financiamiento **PII-DICC-2021-04: *Uso de técnicas de minería de datos para la prevención y detección de ataques a bases de datos por inyección de código SQL***, por una parte, la ***Dra. Alexandra Patricia Alvarado Cevallos*** en calidad de ***Vicerrectora de Investigación, Innovación y Vinculación*** de la Escuela Politécnica Nacional, y por otra la ***Dra. María Asunción Hallo* Carrasco**, en calidad de ***Directora del Proyecto de Investigación Interno sin Financiamiento PII-DICC-2021-04***, al tenor de lo siguiente:

1. ANTECEDENTES

- Mediante Memorando EPN-DICC-2021-0694-M del 9 de septiembre de 2021, la Dra. Rosa del Carmen Navarrete Rueda, presenta al Vicerrectorado de Investigación, Innovación y Vinculación, la propuesta del Proyecto de Investigación Interno sin Financiamiento titulada *Uso de técnicas de minería de datos para la prevención y detección de ataques a bases de datos por inyección de código SQL*.

- El proyecto de Investigación Interno sin Financiamiento *Uso de técnicas de minería de datos para la prevención y detección de ataques a bases de datos por inyección de código SQL*, presentado por la Dra. María Hallo fue aprobado en sesión de Consejo de Investigación, Innovación y Vinculación del 19 de octubre de 2021, mediante Resolución RCIIV-199-2021.

- Con Memorando EPN-VIIV-2021-1928-M del 26 de octubre de 2021, el Vicerrectorado de Investigación, Innovación y Vinculación, notifica a la Jefatura del Departamento de Informática y Ciencias de la Computación que el proyecto de Investigación Interno sin Financiamiento presentado por la Dra. María Hallo ha sido aprobado y que se le ha asignado el código PII-DICC-2021-04, con fecha de inicio el 27 de octubre de 2021 y fecha de fin el 26 de octubre de 2022.

- Mediante Resolución RCIIV-167-2022 del 5 de octubre de 2022 el Consejo de Investigación, Innovación y Vinculación de esta Institución de Educación Superior, en su Décima Séptima Sesión Ordinaria, instalada el 04 de octubre de 2022, por unanimidad resolvió aprobar la solicitud de prórroga técnica del proyecto PII-DICC-2021-04, planteada por la Dra. María Asunción Hallo Carrasco. La nueva fecha de finalización del proyecto en referencia es: 26 de enero de 2023.

Vicerrectorado de Investigación, Innovación y Vinculación
Campus Politécnico "J. Rubén Orellana R." / Av. Ladrón de Guevara E11-253 y Andalucía/ Teléfono: 2976300 Ext. 1050
Quito-Ecuador

2. DATOS GENERALES DEL PROYECTO

Código de Proyecto	PII-DICC-2021-04
Nombre del Proyecto	Uso de técnicas de minería de datos para la prevención y detección de ataques a bases de datos por inyección de código SQL
Director del Proyecto	HALLO CARRASCO MARIA ASUNCION
Colaborador del Proyecto	SUNTAXI OÑA GABRIELA LORENA
Unidad Ejecutora	Departamento de Informática y Ciencias de Computación
Línea de Investigación	Sistemas de Información / Seguridad y Privacidad
Objetivo	Usar de técnicas de minería de datos para la prevención y detección de ataques a bases de datos por inyección de código SQL.
Duración del Proyecto	• Fecha de Inicio: 27 de octubre de 2021 • Fecha de fin planeado: 26 de octubre de 2022 • Fecha fin prórroga técnica :2023-01-26 • Fecha de fin real: 26 de enero de 2023 • Duración total: 15 meses
Entrega del Informe Final	26 de enero de 2023
Entrega del Informe Final corregido	13 de abril de 2023

3. INFORME FINAL:

Mediante Memorandos EPN-PII-DICC-2021-04-2023-0001-M y EPN-PII-DICC-2021-04-2023-0002-M del 26 de enero de 2023, la Dra. María Asunción Hallo Carrasco, Directora del Proyecto de Investigación Interno sin Financiamiento PII-DICC-2021-04, entrega el Informe Final del proyecto que dirige, mismo que es revisado por la Dirección de Investigación, que emite observaciones con memorando EPN-DI-2023-0366-M del 4 de abril de 2023.

La Dra. María Asunción Hallo envía las correcciones al informe final del Proyecto PII-DICC-2021-04, mediante Memorando EPN-PII-DICC-2021-04-2023-0003-M del 13 de abril de 2023. El Informe Final forma parte integrante del Acta de Finalización, cuyas conclusiones y productos generados son:

CONCLUSIONES:

- Se desarrolló un sistema de apoyo para la prevención y detección de ataques a bases de datos por inyección de código SQL usando técnicas de minería de datos demostrando en las pruebas su fiabilidad para cumplir con los objetivos propuestos. Además, se elaboró una guía multimedia con información para prevención y detección de ataques por inyección de código SQL que servirá de apoyo en procesos de enseñanza aprendizaje.

- Para escoger el algoritmo de clasificación que permita detectar anomalías se compararon varios algoritmos usando 633 transacciones y se escogió *k-means* por su facilidad de uso para separar valores normales de valores atípicos y por detectar un mayor número de ataques que fueron correctamente clasificados como valores atípicos. Una vez identificados los valores atípicos se procedió a analizar los textos mediante una función desarrollada para el efecto para encontrar ataques de diferentes tipos: tautologías, ataques basados en consultas ilegales, otros basados en el uso de un operador de unión para conseguir información de bases, tablas y atributos, ataques basados en añadir consultas adicionales, ataques basados en insertar consultas en procedimientos almacenados, otros basados en usar consultas con codificaciones alternativas para evitar controles.

- El modelo fue evaluado usando los indicadores de la matriz de confusión al ejecutar los algoritmos con datos de prueba simulando 100 registros, 50 con comportamiento normal y 50 con anomalías. Los valores de exactitud fueron de 87% y precisión de 89.36%. se realizaron además pruebas de usabilidad con buenos resultados en las encuestas presentadas y pruebas de carga con archivos de diferentes tamaños midiendo el tiempo de ejecución en cada caso variando el tiempo desde 18 segundos para 7000 transacciones a 8673.181 segundos para 7.870.950 transacciones. Se recomienda para el futuro hacer más pruebas con algoritmos para *Big Data*.

- Se puede usar el sistema desarrollado en forma segura como alternativa para detectar ataques por inyección de código SQL. Para prevención la guía desarrollada será de mucha utilidad a los desarrolladores web.

PRODUCTOS:

- **Artículo publicado:** Hallo, M., & Suntaxi, G. (julio 2022). "A survey on SQL injection attacks, detection and prevention techniques – a tertiary study". International Journal of Security and Networks, (Indexada en Scopus Q3) ISN: 1747-8405. DOI: 10.1504/IJSN.2022.125514

- **Artículo publicado:** Chicaiza, C. A., Hallo, M. A., & Suntaxi, G. L. (julio 2022). "Uso de técnicas de minería de datos para la prevención y detección de ataques a bases de datos por inyección de código SQL". (Indexado en Scopus) - Memorias de la CISCI 2022 - Vigésima Primera Conferencia Iberoamericana en Sistemas, Cibernetica e Informatica, Décimo Noveno Simposium Iberoamericano en Educacion, Cibernetica e Informática. DOI: 10.54808/CISCI2022.01.109

- **Trabajo de integración curricular: Ingeniería de Sistemas Informáticos y de Computación:** Añasco, C., & Morocho, K. (octubre 2022). *Desarrollo de un prototipo de sistema que permita la identificación y predicción de ataques a sistemas de bases de datos utilizando técnicas de minería de datos*. URL: http://bibdigital.epn.edu.ec/handle/15000/21809

- **Trabajo de integración curricular: Ingeniería de Sistemas Informáticos y de Computación:** Chicaiza Arévalo, C. A. (agosto 22*). Desarrollo de guía multimedia para detección y prevención de vulnerabilidades en aplicaciones web por inyección de código SQL*. URL: http://bibdigital.epn.edu.ec/handle/15000/22910

- **Trabajo de integración curricular: Ingeniería de Software:** Llumiquinga Guamba, A. M. (octubre 2022). *Evaluación de algoritmos de minería de datos para detección y predicción de Ataques de Inyección SQL en Big Data: Evaluación de SVM para la detección y predicción de Ataques de Inyección SQL en Big Data*. URL: http://bibdigital.epn.edu.ec/handle/15000/23405

- **Trabajo de integración curricular: Ingeniería de Software:** Palma Ponce, B. A. (octubre 2022). *Evaluación de algoritmos de minería de datos para detección y predicción de Ataques de Inyección SQL en Big Data: Evaluación de un Perceptrón Multicapa para la detección y predicción de Ataques de Inyección SQL en Big Data*. URL: http://bibdigital.epn.edu.ec/handle/15000/23400

- **Trabajo de integración curricular: Ingeniería de Software:** Quimbiamba Guasgua, E. J. (octubre 2022). *Evaluación de Algoritmos de Minería de Datos para Detección y Predicción de Ataques de Inyección SQL en Big Data.* URL: http://bibdigital.epn.edu.ec/handle/15000/23401

Otros productos:

- **Ponencia**: Hallo, M. (julio 2022). Ponencia: Guía multimedia para la prevención y detección de vulnerabilidades de inyección SQL durante desarrollo de aplicaciones Web (PyDISQL). En Vigésima Primera Conferencia Iberoamericana en Sistemas, Cibernética e Informática, del 12 al 15 de julio de 2022.

4. LIQUIDACIÓN ECONÓMICA:

El Proyecto de Investigación Interno sin Financiamiento PII-DICC-2021-04, no contó con asignación presupuestaria.

5. FINALIZACIÓN:

Con la presente Acta se declara finalizado y cerrado el Proyecto de Investigación Interno sin Financiamiento PII-DICC-2021-04: *Uso de técnicas de minería de datos para la prevención y detección de ataques a bases de datos por inyección de código SQL*.

Para constancia de lo ejecutado y por estar de acuerdo con el contenido de la presente Acta, las partes libre y voluntariamente suscriben la misma, en tres ejemplares de igual contenido, tenor y valor legal.

Dado en la ciudad de Quito D.M., a los treinta y un días del mes de mayo de dos mil veintitrés.

Firmado electrónicamente por:
ALEXANDRA PATRICIA ALVARADO CEVALLOS

Dra. Alexandra Alvarado
Vicerrectora de Investigación, Innovación y Vinculación

Firmado electrónicamente por:
MARIA ASUNCION HALLO CARRASCO

Dra. María Hallo
Directora del Proyecto PII-DICC-2021-04

xj/np