DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
CARRERA DE INGENIERÍA DE SOFTWARE

TRABAJO DE UNIDAD DE INTEGRACIÓN CURRICULAR, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SOFTWARE

TEMA:

Implementación de un sistema de detección de intrusiones a través de la utilización de honeypots especializados, enfocados en la detección de fraude en tarjetas de crédito y en la monitorización de transacciones, diseñados específicamente para su aplicación en entornos de transacciones en línea.

AUTORES:
CLAUDIO CALVOPIÑA, MARY ELENA
GUAJAN PERUGACHI, JIMMY ISRAEL

DIRECTOR:
Dr. CARRILLO MEDINA, JOSÉ LUIS, Ph.D

LATACUNGA FEBRERO, 2024

Orden del día

- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones

Orden del día

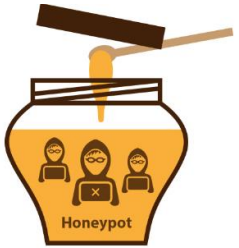
- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones

Problema

- Los ataques cibernéticos, especialmente el fraude con tarjetas de crédito en sistemas de transacciones online, representan una amenaza cada vez mayor.
- Vulnerabilidad de los sistemas de transacciones online ante ataques cibernéticos, especialmente el fraude con tarjetas de crédito.
- Dificultad para tratar estos ataques debido a la evolución constante de las tácticas de los atacantes.

Solución

- Se propone el desarrollo de un honeypot especializado en el estudio del comportamiento de los ataques vinculados al fraude con tarjetas de crédito, integrado en un sistema de ventas online que permite transacciones por internet.
- Se utilizarán modelos y/o algoritmos de Machine Learning, los cuales aprenderán en base a un conjunto de datos que son usadas con frecuencia para detectar el ataque con tarjetas de crédito ya sean clonadas o robadas.



Objetivo General

Desarrollar un sistema de detección de intrusiones a través de la utilización de honeypots especializados, enfocados en la detección de fraude en tarjetas de crédito y en la monitorización de transacciones, diseñados específicamente para su aplicación en entornos de transacciones en línea.

Objetivos Específicos

Investigar el estado del arte sobre el funcionamiento de los honeypots, así como los distintos tipos de honeypots diseñados para rastrear actividades en línea, las técnicas computacionales avanzadas empleadas en su implementación y adquirir un conocimiento detallado acerca de su proceso de desarrollo en un sistema de transacciones online

Implementar un honeypot de tarjetas de crédito que permita detectar el fraude en un entorno de transacciones en línea, y realizar la monitorización de las transacciones completadas.

Validar los resultados, analizar los errores y ajustar el honeypot en un sistema de transacciones online.

- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones

Sistema de Detección de Intrusiones (IPS)

Un sistema de detección de intrusiones es una herramienta de seguridad para redes, donde, ya sea con software o hardware, supervisa actividades maliciosas o detecta violaciones de políticas en una red o sistema Dentro de las funciones y características principales está el monitoreo continuo para observar el tráfico de red y las actividades en los hosts, con el objetivo de detectar (supervisar o identificar) patrones anómalos.

Honeypot

Un honeypot es una herramienta importante para identificar intrusiones en la red. Estos no solo enfrentan al atacante, sino que también recolectan datos que resultan útiles para entender los ataques y a los propios atacantes en la red.

Clasificación de los Honeypots

Honeypots de baja interacción. Son sencillos al momento de su implementación y mantenimiento debido a su capacidad básica requerida de diseño y emulación.

Honeypots de media interacción. Ofrecen una interacción más amplia con los servicios o sistemas implementados, sin llegar a alcanzar las capacidades de los Honeypots de alta interacción.

Honeypots de alta interacción. Se instalan en equipos reales que son accesibles para cualquier usuario dentro de una organización, ya sea en entornos físicos o virtuales

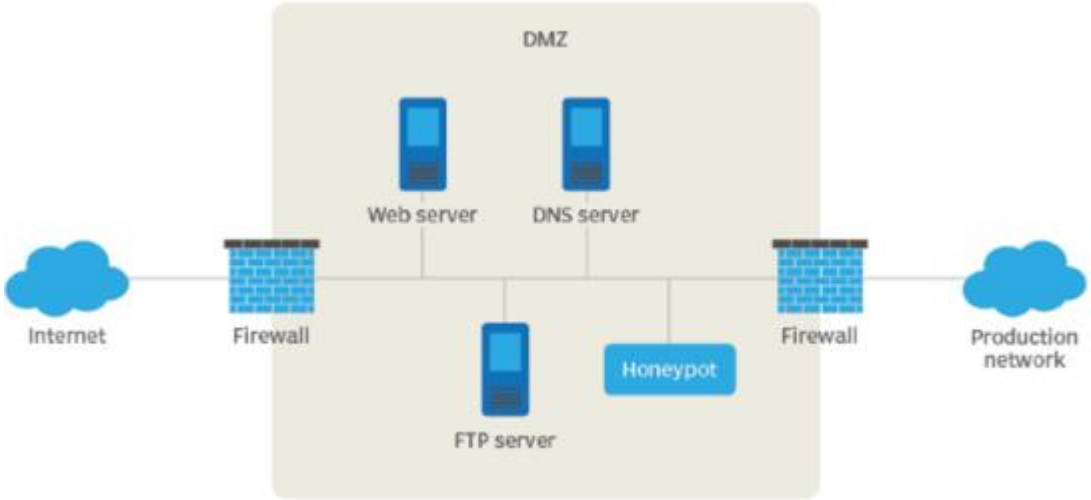
Tipos de Honeypots

Indicadores de ocupación. Las señales de que un honeypot en un sitio web de ventas ha sido ocupado pueden incluir registros de actividad inusuales, picos de tráfico de bots, o intentos de inicio de sesión sospechosos. intentos de acceder a productos o funciones inexistentes.

Honeypots de red. Estos honeypots se configuran en la red y se utilizan para atraer a los atacantes que escanean la red en busca de sistemas vulnerables.

Honeypots de datos. Estos honeypots contienen datos confidenciales, como números de tarjetas de crédito o contraseñas. Se utilizan para atraer a los atacantes que buscan robar datos confidenciales

Ubicación de un honeypot



un honeypot opera mediante una configuración que incluye una computadora, aplicaciones y datos diseñados para imitar el comportamiento de un sistema real, con el propósito de atraer a posibles atacantes

Honeypots en tarjetas de crédito

Los honeypots de datos de tarjetas de crédito son una herramienta de seguridad que se utiliza para recopilar información sobre ciberdelincuentes que intentan robar datos de tarjetas de crédito.

Estos honeypots simulan formularios de entrada en páginas web o aplicaciones que solicitan información de tarjetas de crédito, como números de tarjetas, fechas de vencimiento y códigos de seguridad

Métodos fraude con tarjetas de crédito

El fraude con tarjetas de crédito es uno de los tipos más comunes de fraude de pago y puede incluir el uso no autorizado de tarjetas de crédito o débito para realizar compras, ya sea a través del robo físico de la tarjeta o, más comúnmente, mediante el robo de información de la tarjeta a través de internet

Clonación de Tarjetas de Crédito

La clonación de tarjetas de crédito o débito es un acto ilegal que implica hacer copias no autorizadas de las mismas.

Pérdida de Tarjetas de Crédito

La pérdida o robo de tarjetas de crédito conlleva riesgos significativos de fraude, particularmente en el ámbito de las transacciones en línea

Modelos y/o algoritmos de Machine Learning

Algoritmo de aprendizaje supervisado que se puede utilizar para clasificar las transacciones como legitimas y fraudulentas con una precisión del 91.14%

Decision Tree

Son un conjunto de árboles de decisión entrenados en distintos subconjuntos de datos y features que se puede utilizar para clasificar las transacciones como legitimas y fraudulentas con una precisión del 97.7%

Random Forest

Algoritmo de aprendizaje supervisado que se puede utilizar para clasificar las transacciones como legitimas y fraudulentas con una precisión del 97.4%

Regresión Logística

Algoritmo de aprendizaje supervisado que se puede utilizar para clasificar las transacciones como legitimas y fraudulentas con una precisión del 81.15%

Redes Neuronales

Algoritmo de aprendizaje supervisado que se puede utilizar para clasificar las transacciones como legitimas y fraudulentas con una precisión del 94.5%

Aprendizaje automático basado en reglas

- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones

Análisis del sistema

- Historias de Usuario:

Historia de usuario 01
Quiero un sistema de transacciones en línea enfocados en el pago con tarjetas de crédito.
Para disponer de un sistema enfocado en ventas de productos donde se visualice las páginas para el pago usando tarjetas de crédito.

Análisis del sistema

- Historias de Usuario:

Historia de usuario 02
Quiero que el sistema detecte el fraude en tarjetas de crédito mediante la implementación de honeypots y modelos de machine learning.
Para Usar los modelos con mayor precisión y un honeypot que detecte el fraude en los casos de pérdida o clonación de tarjetas de crédito e identifique los ataques..

Análisis del sistema

- Historias de Usuario:

Historia de usuario 03
Quiero que el sistema permita la monitorización de transacciones emitiendo una alerta al finalizar la transacción y genere un informe de los ataques monitoreados.
Para que el sistema me avise el tipo de transacción como legítima o fraudulenta registrando la transacción.

Lista de Tareas

1

Implementar un sistema de transacciones en línea que acepte solamente pagos con tarjetas de crédito.

2

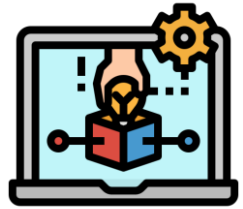
Implementar un honeypot y modelos de machine learning para la detección del fraude en tarjetas de crédito y la monitorización de transacciones..

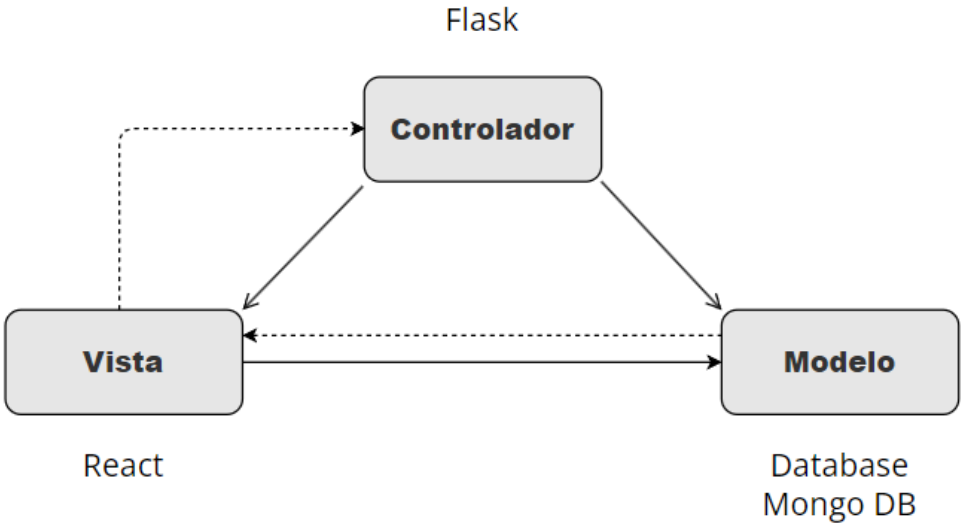
3

Emisión de alerta al finalizar la transacción y generación de un informe de los ataques monitoreados.

Diseño del sistema

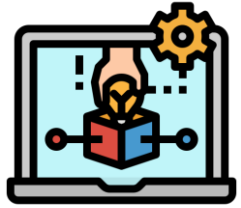
- Arquitectura Lógica con las tecnologías a usar.

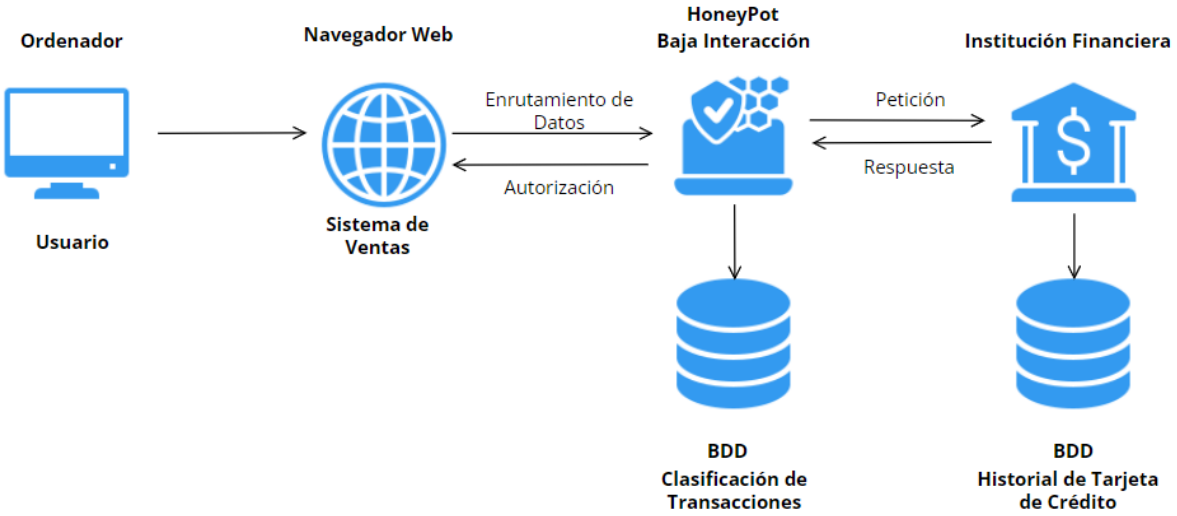




Diseño del sistema

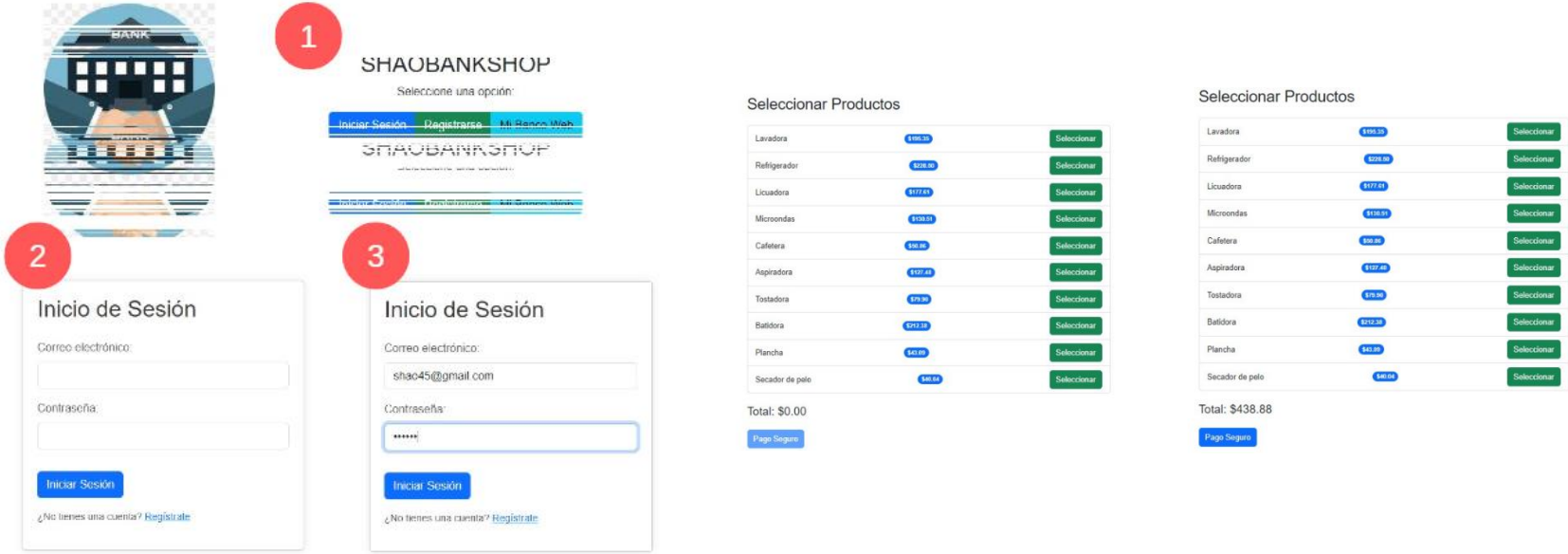
- Arquitectura Física





Diseño del sistema

- Mockups

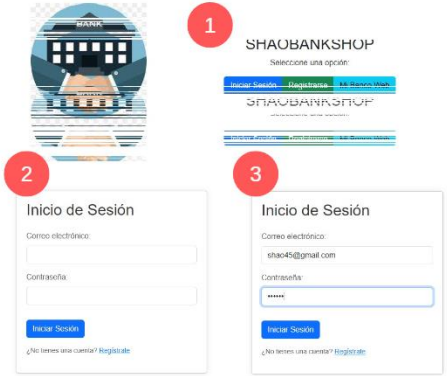


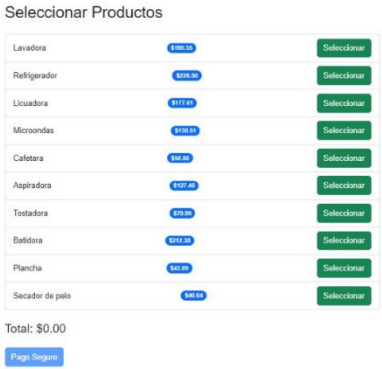
Diseño del sistema

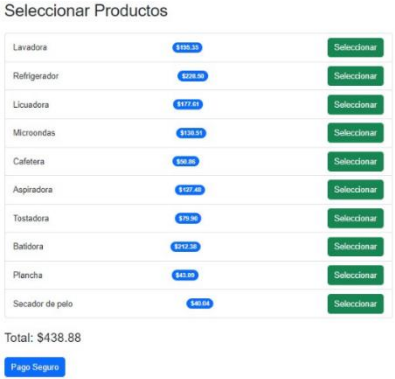
- Mockups

Desarrollo del Sistema

- **Resultado del Sprint 1:** se obtuvo el sistema de transacciones online, primero, para el usuario, se presentan las páginas de Login, ventas, formulario de pago y de la transacción completada..

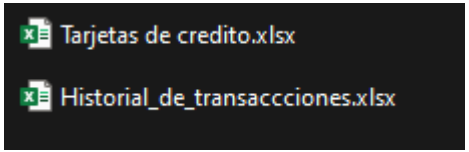






Desarrollo del Sistema

- **Resultado del Sprint 2:** se obtuvo el archivo .CSV, con las características de las tarjetas de crédito y el historial, los cuales serán explicados, a detalle, más adelante. Además, se consiguió la implementación del honeypot y del modelo en el sistema, cumpliendo así con la funcionalidad de la detección de transacciones fraudulentas.



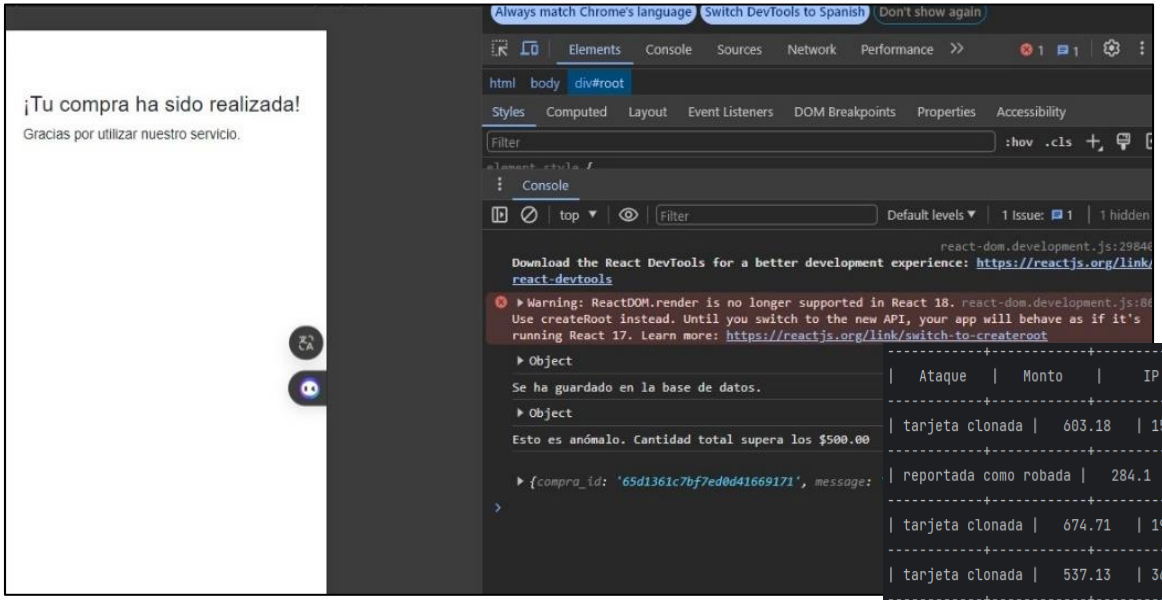

```
Predicción: Verdadero
Predicción: Verdadero
Predicción: Verdadero
Predicción: Verdadero
Predicción: Verdadero
Predicción: Verdadero

Resumen:
Precisión del modelo de Regresión Logística: 0.80
Recall del modelo de Regresión Logística: 1.00
Precisión del modelo de Bosques Aleatorios: 0.68
Recall del modelo de Bosques Aleatorios: 0.80

Process finished with exit code 0
```

Desarrollo del Sistema

- **Resultado del Sprint 3:** se obtuvo el sistema con la implementación de la alerta, además de un informe de ataques que se detallan en los siguientes párrafos.



Ataque	Monto	IP	Puerto	Horario	Tipo	Lugar
tarjeta clonada	603.18	155.59.48.218	5000	12:15	anomalo	Quito
reportada como robada	284.1	204.7.114.107	5000	2:21	anomalo	Latacunga
tarjeta clonada	674.71	192.168.66.230	5000	18:25	anomalo	Guayaquil
tarjeta clonada	537.13	36.226.92.134	5000	1:14	anomalo	Ambato
tarjeta clonada	364.58	192.168.29.142	5000	15:40	normal	Quito
tarjeta clonada	680.24	93.164.120.118	5000	13:4	anomalo	Latacunga

- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones

Validación del Sistema

- Se aplicó validación cruzada, utilizando las funciones cross_val_score() y train_test_split() para evaluar el rendimiento de los modelos de aprendizaje automático de Random Forest y Regresión Logística.

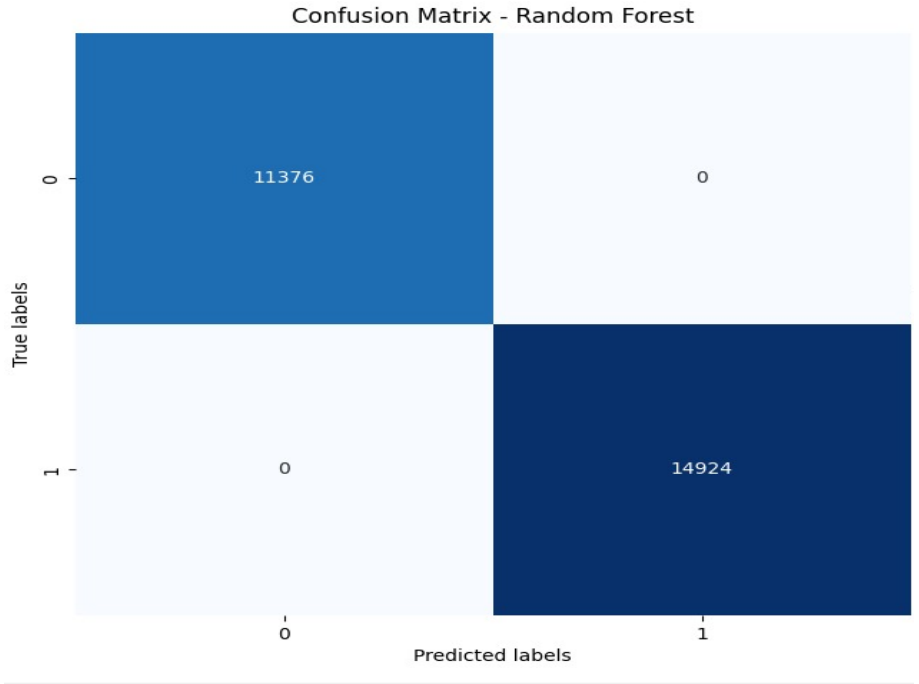
Los resultados obtenidos aplicando validación cruzada durante las cinco iteraciones para el modelo de Random Forest, mostraron los siguientes números presentados, con un promedio de 0.999968

Iteraciones	Acurracy
1	0,999841
2	1
3	1
4	1
5	1
Promedio	0,999968

Validación del Sistema

la matriz de confusión donde se puede visualizar el rendimiento del modelo Random Forest, clasificando los datos en diferentes categorías. En esta matriz, las filas representan las clases reales, mientras que las columnas representan las clases predichas por el modelo.

	Positivos Predicción	Negativos Predicción
Positivos Reales	11376	0
Negativos Reales	0	14924



Análisis de resultados

La matriz de confusión en random forest reflejó un alto número de verdaderos negativos y verdaderos positivos, lo que sugiere una mejora significativa en la capacidad del modelo para identificar correctamente las transacciones anómalas. Sin embargo, en regresión logística, hubo un rendimiento considerablemente menor en comparación al anterior modelo. Aunque el modelo de Regresión Logística logró identificar correctamente la mayoría de las transacciones anómalas, su rendimiento general fue inferior en términos de precisión y exactitud.

Al obtener los resultados de los dos modelos y el honeypot implementado para la detección de fraude en las tarjetas de crédito, Random Forest ha superado a Logistic Regression. Contrastando con el proyecto de fin de grado '*Algoritmos de aprendizaje automático para detección de fraudes con tarjetas de crédito: Análisis y comparativa'* (Calvo Pérez, 2021), el resultado con mayor precisión fue regresión logística, que, con la técnica de submuestreo aleatorio obtuvo un 98,7%, y en el caso de este proyecto, con validación cruzada es de 99,98%.

- Introducción
- Marco Teórico
- Implementación del Sistema
- Validación del Sistema
- Conclusiones

Conclusiones

Se realizó una revisión de la literatura donde se investigó el funcionamiento de los honeypots, así como los distintos tipos de honeypots diseñados para rastrear actividades en línea, encontrando las bases para crear uno de baja interacción, además de las técnicas computacionales avanzadas empleadas en su implementación con los modelos y/o algoritmos de machine learning, se adquirió un conocimiento detallado acerca del proceso de implementación en un sistema de transacciones online.

En un sistema de transacciones online, se implementó un honeypot que detecta el ataque de dos tipos de fraude de tarjetas de crédito: robadas y clonadas. Estableciendo umbrales relacionados a los datos en una transacción. Además, mediante el uso de dos algoritmos de machine learning, Random Forest y Logistic Regression, se consiguió clasificar en transacción anómala o legítima y realizar la monitorización de las transacciones guardando en una base de datos

Conclusiones

Los resultados de los modelos fueron validados, se detectaron los errores que ocasionaron un bajo acurracy, como la omisión de la lectura del campo de lugar, y el reducido número de datos para el entrenamiento, corrigiendo así en el código el análisis del campo y aumentando el número de datos del dataset, de esta forma se implementó el honeypot en un sistema de transacciones online. Logistic Regression presentó una precisión de 0.7847 (78.47%), acurracy de 0.8865 (88.65%) y exhaustividad de 0.6621 (66.21%). Mientras que, Random Forest superó al anterior modelo con una precisión de (0.9998) 99.98%, acurracy de 1.0 (100%) y exhaustividad de 1.0 (100%).

La metodología ha desempeñado un papel crucial en la conclusión exitosa de los objetivos establecidos, gracias a su enfoque iterativo y la importancia que otorga a la retroalimentación constante. Se ha investigado sobre el tema, dividiendo en tres Sprint enfocados en la construcción del sistema de transacciones online. La creación del dataset, la implementación del honeypot y los dos modelos para la detección, para finalmente, emitir alertas y monitorizar las transacciones con un informe. Cumpliendo efectivamente la planificación.

Referencias

- Ahmed, F. (2023). Honeypot. https://forum.huawei.com/enterprise/en/honeypot/thread/668884869385699328-66721385493497036.
- Boukela, L., Zhang, G., Bouzefrane, S., & Zhou, J. (2020). An outlier ensemble for unsupervised anomaly detection in honeypots data. Intelligent Data Analysis, 24(4), 743-758. Scopus. https://doi.org/10.3233/IDA-194656
- González, A. (2021). *Honeypot, análisis e implementación. Análisis de resultados y aplicación práctica* [Universidad de Almería]. https://repositorio.ual.es/bitstream/handle/10835/13521/GONZALEZ%20LOZANO,%20ANTONIO%20JESUS.pdf?sequence=1&isAllowed=y

Software
DOMINA EL MUNDO

Gracias por su atención

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA