Kevin Julian Neisa Gonzalez – 20222020224 – Comparacion de metodologias

A Review on Phishing Threats and Data Securityin Online Trading Systems using Artificial Intelligence Techniques

Metodología del artículo

El estudio realizado por Murugun et al. (2024) se basa en un enfoque de revisión sistemática de literatura para analizar las amenazas de phishing y las estrategias de seguridad de datos en sistemas de comercio en línea mediante técnicas de inteligencia artificial (IA). La metodología comprende los siguientes pasos:

1. Selección y recopilación de literatura
   Se identificaron estudios relevantes sobre phishing y detección mediante IA, abarcando investigaciones recientes relacionadas con clasificación de phishing, aprendizaje automático, aprendizaje profundo, procesamiento de lenguaje natural (NLP) y entrenamientos de concienciación en ciberseguridad.
2. Categorización de técnicas y enfoques
   Los estudios recopilados fueron clasificados según la metodología utilizada, incluyendo:
   - Algoritmos de aprendizaje automático supervisado y no supervisado.
   - Modelos de aprendizaje profundo, como redes neuronales convolucionales (CNN) y recurrentes (RNN).
   - Técnicas de procesamiento de lenguaje natural (NLP) para detección de phishing en correos electrónicos.
   - Métodos de entrenamiento en ciberseguridad basados en IA para concienciación de usuarios.
3. Análisis comparativo
   Se evaluaron los métodos según métricas de desempeño como precisión, recall, F1-score y exactitud. También se analizaron los desafíos de cada técnica, incluyendo disponibilidad de datos, interpretabilidad del modelo y escalabilidad.
4. Síntesis de resultados y hallazgos
   Se elaboró un resumen de los enfoques más eficaces para la detección de phishing, destacando:
   - La efectividad de los modelos ensemble y combinaciones de múltiples algoritmos.
   - La importancia del entrenamiento de usuarios para reducir vulnerabilidades humanas.
   - Las limitaciones de cada técnica y los retos futuros, como la adaptación en tiempo real y la integración de métodos múltiples.

5. Propuestas para investigación futura
   Se identificaron áreas de mejora y nuevas líneas de investigación, incluyendo:
   - Integración de distintos enfoques de IA para detección proactiva.
   - Mejora en la interpretación y robustez de los modelos.
   - Colaboración entre stakeholders para fortalecer la seguridad en sistemas de comercio electrónico.

En resumen: la metodología es un análisis sistemático y comparativo de estudios previos, basado en revisión de literatura, categorización de técnicas de IA, evaluación de desempeño y síntesis de resultados con recomendaciones para futuras investigaciones.

STATISTICAL PROSPECTS OF ARTIFICIAL INTELLIGENCE IN TACKLING CYBER CRIMES

Metodología del estudio:

El estudio se centra en analizar cómo las técnicas de inteligencia artificial (IA) pueden aplicarse para prevenir y detectar delitos cibernéticos. La investigación sigue un enfoque descriptivo y analítico basado en la revisión bibliográfica y el análisis estadístico de factores relacionados con los cibercrímenes.

1. Recolección de información:
   Se recopilan datos de fuentes académicas, técnicas y estadísticas sobre cibercrimen, incluyendo casos de ataques informáticos, fraudes en línea y vulnerabilidades en redes.
2. Clasificación de cibercrímenes y factores asociados:
   Se identifican y categorizan diferentes tipos de cibercrímenes y los factores que los facilitan, como la autenticación, control de acceso, alerta y recopilación de información sobre amenazas.
3. Aplicación de técnicas de inteligencia artificial:
   Se evalúa el uso de diversas técnicas de IA, incluyendo:
   - Redes neuronales artificiales (ANN) para detección de intrusiones y clasificación de malware.
   - Agentes inteligentes para la coordinación y respuesta ante ataques en tiempo real.
   - Sistemas inmunes artificiales (AIS) para identificar patrones de comportamiento anómalo y ataques de Botnets.
   - Algoritmos genéticos y lógica difusa (fuzzy) para optimizar la detección de anomalías y ataques de red.
4. Análisis estadístico:
   Se realiza un análisis ANOVA y diagnóstico de colinealidad para establecer relaciones entre

los factores de seguridad y la incidencia de cibercrímenes, evaluando la significancia estadística de los predictores seleccionados.

5. Evaluación de sistemas de detección y prevención:
   Se examinan sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IDPS) basados en IA, identificando sus fortalezas, limitaciones y aplicabilidad práctica en entornos de seguridad informática.
6. Síntesis y discusión:
   Los resultados obtenidos de la literatura y los análisis estadísticos se integran para proporcionar un panorama de la efectividad de las técnicas de IA frente a cibercrímenes, destacando las áreas de mayor aplicabilidad y las limitaciones actuales.

Design Challenges for Scam Prevention Tools to Protect Neurodiverse and Older Adult Populations

Metodología

El presente estudio adoptó un enfoque de revisión crítica de literatura para identificar los desafíos en el diseño de herramientas de prevención de estafas dirigidas a poblaciones neurodiversas y adultos mayores. La metodología se estructuró en las siguientes fases:

1. Selección de literatura relevante: Se recopilaron publicaciones académicas y técnicas de diversas fuentes confiables, incluyendo revistas indexadas, conferencias internacionales y reportes institucionales. La búsqueda se centró en tres dominios principales:
   - Desafíos y necesidades de individuos con diversas discapacidades (físicas, sensoriales, cognitivas, de comunicación y neurodiversas).
   - Herramientas y tecnologías de asistencia aplicadas en contextos educativos y digitales.
   - Soluciones de ciberseguridad actuales, con énfasis en la inclusión y accesibilidad.
2. Categorización y análisis de desafíos: Los datos obtenidos fueron clasificados según el tipo de discapacidad y los obstáculos específicos que enfrentan los usuarios al interactuar con sistemas de seguridad digitales. Se identificaron brechas de accesibilidad, limitaciones cognitivas y sesgos potenciales en modelos de inteligencia artificial utilizados en herramientas de detección de estafas.
3. Síntesis de enfoques de diseño inclusivo: Se analizaron ejemplos de tecnologías de asistencia y diseños inclusivos en otros dominios, particularmente en educación y aprendizaje asistido por IA. Esto permitió extraer principios aplicables a la creación de interfaces adaptativas y mecanismos de alerta personalizados para la prevención de estafas.

4. Propuesta del marco inclusivo: Con base en el análisis de literatura y los principios de diseño inclusivo, se desarrolló el Inclusive AI-driven Cybersecurity (IAC) Framework. Este marco integra técnicas de inteligencia artificial para la mitigación de ataques de ingeniería social, considerando la diversidad de necesidades cognitivas, sensoriales y de interacción de los usuarios.

5. Retroalimentación y mejora continua: La metodología incorpora la noción de loops de retroalimentación, los cuales permitirían, en fases futuras de implementación, ajustar los modelos de IA y las interfaces según la experiencia de los usuarios, reduciendo sesgos y mejorando la efectividad y accesibilidad del sistema.

En conjunto, este enfoque metodológico permite comprender las limitaciones de las soluciones existentes y establecer un marco de diseño inclusivo para herramientas de prevención de estafas, con un énfasis particular en poblaciones vulnerables, garantizando tanto la eficacia de la detección de estafas como la accesibilidad del sistema para todos los usuarios.

ElderConnect: An AI-Powered Platform to Empower Seniors Against Cyberthreats

Metodología del artículo

El estudio desarrolla ElderConnect, una plataforma de concienciación y apoyo en ciberseguridad para adultos mayores, integrando inteligencia artificial (IA), aprendizaje automático y talleres prácticos. La metodología se centra en dos componentes principales: el chatbot de IA y la detección de URLs falsas.

A. Chatbot de IA

1. Selección del modelo:
   Se seleccionó el modelo LLaMA 3.1 por su capacidad para comprender patrones lingüísticos complejos y generar respuestas contextualmente apropiadas, optimizando la asistencia en tiempo real ante amenazas cibernéticas.

2. Ajuste fino (fine-tuning):
   El modelo pre-entrenado se adaptó a un conjunto de datos específico de ciberseguridad, que incluyó discusiones técnicas, preguntas frecuentes y terminología del dominio. La optimización se realizó mediante aprendizaje supervisado y validación con un conjunto de datos separado para asegurar precisión y relevancia en las respuestas.

3. Uso de datos estructurados de Hugging Face:
   Los datos de entrenamiento se obtuvieron de Hugging Face, incluyendo preprocesamiento de textos y tokenización compatible con LLaMA 3.1, garantizando entradas coherentes y de alta calidad para el aprendizaje.

4. Optimización del modelo:
   Se aplicaron técnicas de ajuste de hiperparámetros, cuantización y poda del modelo para

reducir complejidad computacional y mejorar la velocidad de respuesta sin sacrificar la precisión.

5. Despliegue mediante Ollama:
   El chatbot se implementó utilizando Ollama, con contenedorización en Docker para escalabilidad y herramientas de monitoreo en tiempo real que permiten seguimiento del desempeño y recopilación de datos de interacción.

6. Interacción contextual:
   Se incorporó un mecanismo de memoria que permite al chatbot recordar conversaciones previas, ofreciendo respuestas coherentes y personalizadas, y asegurando continuidad en la asistencia al usuario.

B. Detección de URLs falsas

1. Selección de modelos:
   Se implementó un conjunto de algoritmos de aprendizaje automático y profundo para maximizar la efectividad en la detección de phishing:
   - SVM: clasificación binaria de URLs seguras o maliciosas.
   - CNN: reconocimiento de patrones complejos en la estructura de URLs.
   - GRNN: adaptabilidad a cambios graduales en ataques emergentes.
   - Regresión logística: asignación de puntaje de riesgo a URLs.
   - GRU y BiLSTM: captura de dependencias temporales en secuencias de URLs.
   - BERT: análisis de atributos textuales de URLs y detección de anomalías lingüísticas.

2. Evaluación de modelos:
   Se evaluaron los modelos usando métricas de desempeño como accuracy, precision, recall y F1-score, asegurando la detección confiable de URLs maliciosas.

3. Integración de Explainable AI (XAI):
   Se incorporaron técnicas de XAI para mejorar la transparencia y confianza en las predicciones del sistema.

C. Talleres y educación práctica

- Se organizaron talleres comunitarios para adultos mayores, combinando presentaciones sobre amenazas reales y ejercicios prácticos usando el chatbot, herramientas de verificación de URLs y detección de perfiles falsos.
- Cada sesión incluyó análisis de correos y enlaces sospechosos, aumentando la confianza y precisión de los participantes en la detección de fraudes.
- Los talleres se complementaron con guías impresas y un entorno de chat comunitario seguro para reforzar el aprendizaje.

Cyber Fraud Economics, Scam Types, and Potential Measures to Protect U.S. Seniors: A Short Review

Metodología

El estudio se desarrolló mediante un análisis de revisión bibliográfica enfocado en el fraude cibernético dirigido a adultos mayores en Estados Unidos. La metodología consistió en:

1. Selección de fuentes y referencias:
   Se recopilaron informes de agencias gubernamentales (FTC, GAO, NCEA, SSA), bases de datos académicas y literatura científica, así como artículos de medios especializados sobre fraudes a adultos mayores.
2. Clasificación de la información:
   Se organizaron los hallazgos en categorías temáticas:
   - Tipos de fraudes (sweepstakes, soporte técnico, romance, phishing, robo de identidad, sobrepagos).
   - Vectores de propagación (llamadas de voz, correos electrónicos, SMS, cartas, pop-ups).
   - Tácticas avanzadas (uso de inteligencia artificial, ingeniería social, encuestas fraudulentas).
   - Señales de alerta y patrones de comportamiento de las víctimas.
3. Síntesis de medidas preventivas y recursos:
   Se identificaron estrategias de mitigación y prevención a partir de literatura y guías oficiales, incluyendo:
   - Buenas prácticas de ciberseguridad (contraseñas seguras, autenticación multifactor, antivirus, bloqueadores de pop-ups, aplicaciones de no llamar).
   - Recursos disponibles para adultos mayores y sus cuidadores para reportar y prevenir fraudes.
4. Presentación de resultados:
   Los datos se resumieron en forma de gráficos estadísticos, tablas de recursos y descripciones narrativas de las tácticas de fraude y sus medidas preventivas.

En síntesis, la metodología adoptada fue de tipo revisión documental descriptiva, integrando fuentes secundarias oficiales y académicas, con el objetivo de proporcionar una visión integral sobre los fraudes cibernéticos a adultos mayores, sus vectores, tácticas y posibles estrategias de mitigación.

Comparación de las 5 metodologías

Observaciones generales comparativas:

1. Enfoque técnico vs. socioeducativo:
    - Los estudios de *phishing* y *statistical AI* son más técnicos, centrados en IA, modelos de detección y análisis estadístico.
    - Los estudios *ElderConnect*, *Design Challenges* y *Cyber Fraud Economics* son más aplicados a la protección de adultos mayores, con énfasis en educación, accesibilidad y mitigación práctica.
2. Tipo de datos:
    - *Phishing* y *Statistical AI* usan datasets técnicos y literatura científica.
    - *ElderConnect* combina datasets con datos de interacción real de usuarios.
    - *Cyber Fraud Economics* y *Design Challenges* se basan en literatura, reportes y casos reales, no en datasets de ML.
3. Nivel de aplicación:
    - *ElderConnect* es el único que implementa un sistema funcional y talleres prácticos.
    - *Design Challenges* propone un marco conceptual inclusivo.
    - Los demás son revisiones y análisis de literatura.
4. Innovación:
    - *Phishing* y *Statistical AI* destacan en técnicas avanzadas de IA.
    - *ElderConnect* combina IA con educación práctica.
    - *Design Challenges* resalta diseño inclusivo y adaptativo.
    - *Cyber Fraud Economics* aporta enfoque preventivo y de recursos para adultos mayores.