**Sistematización del Tema de Investigación**

**Línea de Investigación**

Inteligencia Artificial aplicada a la Ciberseguridad.

**Tema General**

Seguridad en Servidores

**Temas Particulares**

Logs de autenticación de Seguridad en Servidores

Tráfico de red para Seguridad en servidores

Comportamiento de usuarios para Seguridad de servidores

**Temas Específicos**

Mala detección de patrones de ataques de fuerza bruta en los logs de autenticación de seguridad en servidores.

Identificación de comportamientos de acceso anómalo en los logs de autenticación de seguridad en servidores.

Clasificación de actores de amenaza a partir de los logs de autenticación de seguridad en servidores.

**Problema de Estudio**

Mala detección de patrones de ataques de fuerza bruta en los logs de autenticación de seguridad en servidores, 2025

**Título Preliminar de la Tesis**

Detección de patrones de ataques de fuerza bruta en los logs de autenticación de seguridad en servidores, 2025

**Variable Dependiente:** detección de patrones de ataques de fuerza bruta

**Objeto de Estudio:** logs de autenticación

**Alcance Espacial:** seguridad en servidores

**Alcance Temporal:** 2025

**Antecedentes Bibliográficos**

Bajramovic, E., Fein, C., Frinken, M., Rösler, P., & Freiling, F. (2023). LAVA: Log Authentication and Verification Algorithm. *Digital Threats: Research and Practice, 4*(3), 1–17. <https://doi.org/10.1145/3609233>

Flynn, R., & Olukoya, O. (2025). Using approximate matching and machine learning to uncover malicious activity in logs. *Computers & Security, 151*, 104312. <https://doi.org/10.1016/j.cose.2025.104312>

Gudivaka, B. R., Gudivaka, R. L., Gudivaka, R. K., Basani, D. K. R., Grandhi, S. H., Murugesan, S., & Kamruzzaman, M. M. (2025). A predominant intrusion detection system in IIoT using ELCG-DSA AND LWS-BIOLSTM with blockchain. *Sustainable Computing: Informatics and Systems, 46*, 101127. <https://doi.org/10.1016/j.suscom.2025.101127>

Islam, M. E., Islam, M. R., Chetty, M., Lim, S., & Chadhar, M. (2023). User authentication and access control to blockchain-based forensic log data. *EURASIP Journal on Information Security, 2023*(7). <https://doi.org/10.1186/s13635-023-00142-3>

Krishna, D. P., Ramaguru, R., Praveen, K., Sethumadhavan, M., Ravichandran, K. S., Krishankumar, R., & Gandomi, A. H. (2023). SSH-DAuth: Secret sharing based decentralized OAuth using decentralized identifier. *Scientific Reports, 13*(1), 18335. <https://doi.org/10.1038/s41598-023-44586-6>

**Título Tentativo de la Tesis**

Framework basado en inteligencia artificial para mejorar la detección de patrones de ataques de fuerza bruta en los logs de autenticación de seguridad en servidores, 2025

**Variable Independiente:** Framework basado en inteligencia artificial

**Variable Dependiente:** Detección de patrones de ataques de fuerza bruta

**Objeto de Estudio:** Logs de autenticación

**Alcance Espacial:** Seguridad en servidores

**Alcance Temporal:** 2025

**ANEXO 1: MATRIZ DE CONSISTENCIA**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Título:** Framework basado en inteligencia artificial para mejorar la detección de patrones de ataques de fuerza bruta en los logs de autenticación de seguridad en servidores, 2025 | | | | | | |
| **LINEA DE**  **INVESTIGACIÓN** | **PROBLEMA DE ESTUDIO** | **PROBLEMAS** | **OBJETIVOS** | **HIPÓTESIS** | **VARIABLES Y DIMENSIONES** | **DISEÑO**  **METODOLÓGICO** |
| Inteligencia Artificial aplicada a la Ciberseguridad. | Mala detección de patrones de ataques de fuerza bruta en los logs de autenticación de seguridad en servidores, 2025 | **Problema general:**  ¿De qué manera un framework basado en inteligencia artificial mejora la detección de patrones de ataques de fuerza bruta en los logs de autenticación de seguridad en servidores, 2025? | **Objetivo general:**  Determinar la mejora que produce un framework basado en inteligencia artificial en la detección de patrones de ataques de fuerza bruta en los logs de autenticación de seguridad en servidores, 2025. | **Hipótesis general:**  El framework basado en inteligencia artificial mejora significativamente la detección de patrones de ataques de fuerza bruta en los logs de autenticación de seguridad en servidores. | **Variable independiente:** Framework basado en inteligencia artificial (Cuantitativo)  **Dimensiones**  - Arquitectura del Modelo - Procesamiento y Representación de Datos de Logs  -Eficiencia y Características Operacionales del Framework | **Enfoque:** Cuantitativo  **Tipo de**  **Investigación:**  Aplicada  **Nivel de**  **Investigación:**  Correlacional  **Diseño:**  Experimental, Transversal |
| **OBJETO DE ESTUDIO** |
| Logs de autenticación | **Problemas específicos:** | **Objetivos específicos:** | **Hipótesis específicas:** | **Variable dependiente:** |  |
| PE1: ¿De qué manera la arquitectura del modelo del framework basado en inteligencia artificial se relaciona con la detección de patrones de ataques de fuerza bruta en los logs de autenticación?  PE2: ¿Cuál es la relación entre el procesamiento y representación de datos de logs del framework y la detección de patrones de ataques de fuerza bruta en los logs de autenticación?  PE3: ¿Cómo influye la eficiencia y las características operacionales del modelo en la detección de patrones de ataques de fuerza bruta en los logs de autenticación? | OE1: Evaluar la relación entre la arquitectura del modelo del framework y la mejora en la detección de patrones de ataques de fuerza bruta.  OE2: Analizar la relación que existe entre el procesamiento y representación de datos de logs del framework y la mejora en la detección de patrones de ataques de fuerza bruta.  OE3: Medir la influencia de la eficiencia y las características operacionales del framework en la mejora de la detección de patrones de ataques de fuerza bruta. | HE1: La arquitectura del modelo del framework se relaciona directa y positivamente con la mejora en la detección de patrones de ataques de fuerza bruta.  HE2: El procesamiento y la representación de datos de logs del framework se relacionan directa y positivamente con la mejora en la detección de patrones de ataques de fuerza bruta.  HE3: La eficiencia y las características operacionales del framework se relacionan directa y positivamente con la mejora en la detección de patrones de ataques de fuerza bruta. | Detección de patrones de ataques de fuerza bruta (Cuantitativo)  **Dimensiones**  - Puntuación de Similitud (Similarity Score) - Distancia Hamming (Hamming Distance) -Resistencia a la Truncación () - Tiempo de Retención de Datos (en meses o años) |