Universidad Nacional de La Pampa
Facultad de Ingeniería
Laboratorio de Investigación en Sistemas Inteligentes

Universidad Nacional de La Pampa

Detección de Ransomware en Blockchains

Proyecto: Big data optimization con algoritmos metaheurísticos utilizando frameworks de computación distribuida

Directora: Carolina Salto
Investigadores: Yanina Ditz, Gabriela Minetti

Resumen

El *ransomware* es un tipo de *malware* (código malicioso) que bloquea el acceso a los datos de un dispositivo, hasta que se pague un rescate, el cual se hace en Bitcoin. A partir de este problema ,surgen sistemas para la detección de esto código malicioso como el modelo topológico del análisis de datos y técnicas de minerías de datos. Mediante el estudio de estas herramientas se profundiza en la implementación y análisis de redes neuronales para aprender a reconocer patrones y comportamientos comunes en las transacciones de Bitcoins.

Introducción

Un poco de historia

En el año 2005, aparece el primer *ransomware* moderno, pero es en el 2008, con la aparición del Bitcoin, que este delito entra en auge. Al finalizar el año 2015, el FBI estimó que las víctimas pagaron 27 millones de dólares a los atacantes.

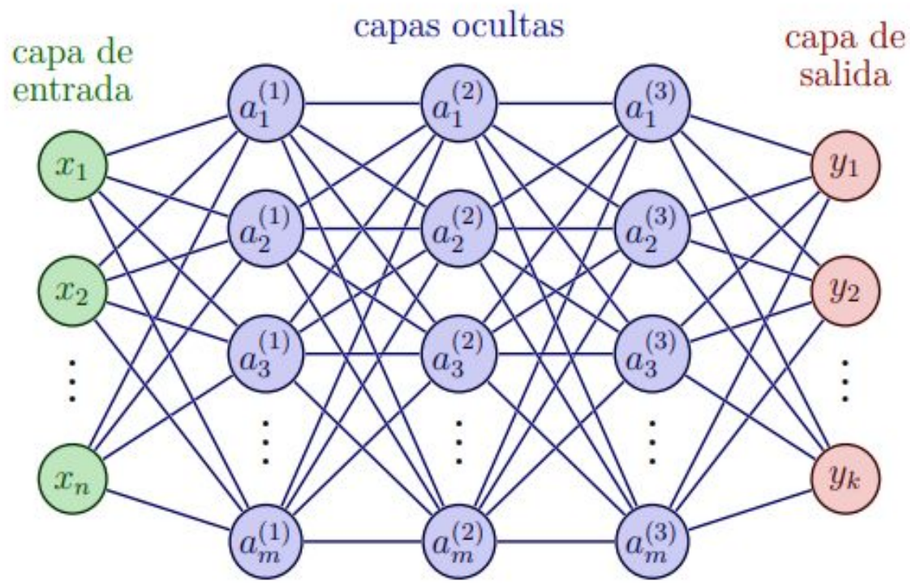
Por ende, la detección de *ransomware* es tan importante y este proceso requiere de métodos que permitan manejar, analizar y obtener información de cada transacción de Bitcoin para identificar direcciones fraudulentas. Dicha identificación se lleva a cabo a través de diferentes técnicas que realizan tareas como seleccionar y extraer datos, procesarlos, obtener su valor, visualizarlos y presentarlos. Dentro de las cuales se encuentran el modelo topológico del análisis de datos para extraer patrones y las técnicas de minería de datos y aprendizaje automático para el estudio del sistema dinámico de detección de *ransomware.*

Desarrollo

Nuestro trabajo

Para la detección dinámica de *ransomware* en *Blockchain* de Bitcoins se espera adaptar una red neuronal, que permita:

1. mejorar el rendimiento de la misma, al aumentar el conjunto de datos sin clasificar;
2. resolver las limitaciones de los datos categorizados, ya sea orgánica o sintéticamente, al incrementar las categorías submuestradas;
3. introducir técnicas automáticas para la reducción de la dimensionalidad;
4. normalizar los atributos; y
5. ajustar los parámetros de los algoritmos.



Formación de Recursos Humanos

Con esta línea de investigación se propende a la formación, de la primera autora, en investigación siguiendo el método científico, llevando a cabo gran parte de la investigación requerida en su tesis de maestría.

ISI