International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 03 | March - 2023 Impact Factor: 7.185 ISSN: 2582-3930

# Ransomware Detector Using Artificial Neural Network

BHUKYA RAJA KUMAR[1],T GAYATHRI[2], P THOUHITH KHAN[3],
M LAKSHMI VARAPRASAD[4], G SANJAY KRISHNA[5]
[1]Assitant professor, [2,3,4,5] Students, Dept of CSIT
[1,2,3,4,5] Siddharth Institute of Engineering & Technology, Puttur-517583

---

**Abstract -** This design demonstrates a new approach to detecting ransomware targeted at Microsoft Windows, combining 2 deep literacy neural network classifiers to produce an ensemble, taking lines as input in Microsoft's standard PE train format, similar as those with a '. exe ' train extension, and returning a vaticination of the train belonging to 1 of 3 classes benign, general malware, or ransomware. The model's capability to distinguish between ransomware and other forms of malware allows it to be applied as an extension to a being malware discovery system similar as anti-virus software, and aid in the categorization and rear engineering of new in- the-wild ransomware samples. The results of testing the ensemble model on data not seen in its training suggest a high position of prophetic power in classifying new in- the-wild samples.

Keywords: Ransomware, Malware, Windows

## Introduction

Ransomware is a malware type that is designed to prevent or reduce access a user has to their device, operating system, or files. Ransomware is typically found in the forms of locker ransomware and crypto-ransomware. Locker ransomware displays a lock screen that prevents the victim from accessing their computers, often pretending to be law enforcement demanding monetary payment in return for access to the computer. Crypto-ransomware encrypts key files on a user's system, using complex encryption schemes and demand fees, usually in the form of crypto currency to decrypt the victim's files. The decision to evaluate machine learning and deep learning approaches as opposed to other non-machine learning-based approaches was taken because of their adaptability and strong ability to detect unseen samples of ransomware malware. Non-learning approaches tend to warrant the capability to acclimatize or be retrained to a new conception snappily. These approaches would take significantly more time to recalibrate. We have an interest in the possible wide-scale integration of these solutions in IoT (Internet of Things) to prevent the infection of IoT devices.

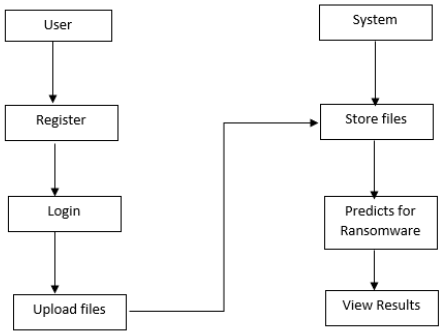
## SCOPE:

This application can be extended to include the ability to predict multiple anti-virus and security issues. we plan to explore the prediction methodology using the updated viruses and use the most accurate and appropriate methods for predicting.

**Related Work**

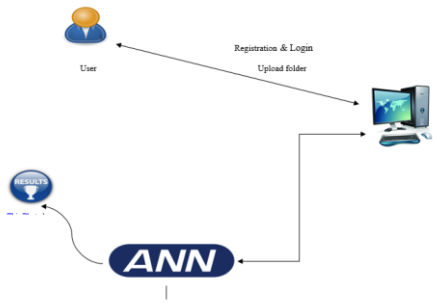
**1.Proposed Work**

We propose this application that can be considered a useful system since it helps to reduce the limitations obtained from KNN and Logistic Regression. By providing support through the regression analysis, it can be able to generate best results for attributes without any overlap. The system is developed in a Flask based Python environment.




MySQL is used for database management and the models involved in this application are artificial neural network ANN.

**2. Model Architecture**




**PE file**

The system art he Portable Executable (PE) format may be a file format for executable, code, DLLs, FON Font files, et al. utilized in 32-bit and 64-bit versions of Windows operating systems. The PE format may be an arrangement that encapsulates the knowledge necessary for the Windows OS haul to handle the banded executable law. This includes energetic archive sources for associating, API import and import tables, resource operation data and thread-original storehouse( TLS) data. On NT operating systems, the PE formation is assumed for EXE, DLL, SYS( device motorist), and different train kinds. The Extensible Firmware Interface( EFI) specification states that PE is that the common executable formation in EFI terrain.

**PE HEADER**

The PE train title consists of a Microsoft MS-DOS end, the PE hand, the COFF train title, and an elective title. A COFF thing train title consists of a COFF train title and an elective title. In both cases, the train heads are succeeded incontinently by neighborhood heads.

- MS-DOS Stub (Image Only)
- Signature (Image Only)
- COFF File Header (Object and Image)
- Machine Types
- Characteristics
- Optional Header (Image Only)
- Optional Header Standard Fields (Image Only)
- Optional Header Windows-Specific Fields (Image Only)
- Optional Header Data Directories (Image Only)

## 2. Algorithm

### 2.1.Artificial neural networks (ANNs)

Artificial neural networks (ANNs), usually simply called neural networks (NNs), are computing systems vaguely inspired by the biological neural networks that constitute animal brains An ANN is predicated on a collection of connected units or bumps called artificial neurons, which roughly model the neurons in a natural brain. Each connection, like the synapses in a biological brain, can transmit a signal to other neurons. An artificial neuron that receives a signal then processes it and can signal neurons connected to it. The "signal" at a connection is a real number, and the output of each neuron is computed by some non-linear function of the sum of its inputs. The connections are called edges. Neurons and edges typically have a weight that adjusts as learning proceeds. .The weight increases or decreases the strength of the signal at a connection. Neurons may have a threshold such that a signal is sent only if the aggregate signal crosses that threshold. Typically, neurons are aggregated into layers. Different layers may perform different transformations on their inputs. Signals travel from the first caste( the input caste), to the last caste( the affair caste), possibly after covering the layers multiple times.

### 2.2.Tensor Flow

TensorFlow is a free and open- source software library for machine literacy. It can be used across a range of tasks but has a particular focus on training and conclusion of deep neural networks.( TensorFlow is a emblematic calculation library grounded on dataflow and differentiable programming. It's used for both exploration and product at Google. TensorFlow was developed by the Google Brain platoon for internal Google use. It was released undergoing the Apache License2.0 in 2015. TensorFlow is Google Brain's alternate- generation system. Version1.0.0 was released on February 11, 2017.( 14) While the reference perpetration runs on single bias, TensorFlow can run on multiple CPUs and GPUs( with voluntary CUDA and SYCL extensions for general- purpose computing on plates recycling units).( 15) TensorFlow is available on 64- bit Linux, macOS, Windows, and mobile computing platforms including Android and iOS. Its flexible armature allows for the easy deployment of calculation across a variety of platforms( CPUs, GPUs, TPUs), and from desktops to clusters of waiters to mobile and edge bias. TensorFlow calculations are written as stateful dataflow graphs. The name TensorFlow derives from the operations that similar neural networks perform on multidimensional data arrays, which are appertained to as tensors. During the Google I/ O Conference in June 2016, Jeff Dean stated that,500 depositories on GitHub mentioned TensorFlow, of which only 5 were from Google.

**Procedure:**

- Import all the Libraries/packages.
- Perform Exploratory data analysis.
- Train the folders neural networks algorithms mentioned and record their accuracies.
- The model is used for prediction of performance from the data.

**4. Result:**

The Experimental Results detail is given below:

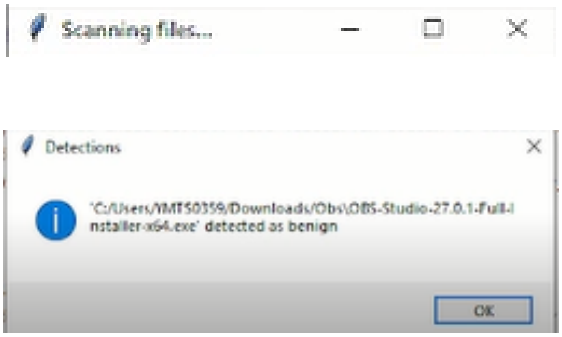



Fig : Scanning files

Fig : Result of the project

**5. Conclusion:**

In this application, we have successfully created a system to prediction whether the uploaded folder contains Ransomware or not. This is developed in a user-friendly environment using Flask via Python programming. The system is likely to collect information from the user to predict the requirements.

**6. References:**

1.A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques Damien Warren Fernando 1,* , Nikos Komninos 1and Thomas Chen 21Department of Computer Science, City, University of London, London EC1V 0HB, UK;Nikos.Komninos.1@city.ac.uk2Department of Electrical and Electronic Engineering, City, University of London, London EC1V 0HB, 29 September 2020; Accepted: 11 December 2020; Published: 15 December 2020.

2.Ransomware Detection Using the Dynamic Analysis and Machine Learning A check and exploration Directions by Umara Urooj 1, *, Bander Ali Saleh Al- rimy 1, Anazida Zainal 1ORCID, FuadA. Ghaleb 1ORCID andMuradA. Rassam,3 ORCID School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, Johor Bahru 81300, Johor, Malaysia Department of Information Technology, College of Computer, Qassim University, Buraydah 51452, Saudi Arabia Faculty of Engineering and Information Technology, Taiz University, Taiz 6803, Yemen * Author to whom correspondence should be addressed. Appl.Sci. 2022, 12( 1), 172; https//doi.org/10.3390/app12010172Received 26 November 2021 Revised 21 December 2021/ Accepted 21 December 2021/ Published 24 December 2021.

3.Ransomware Detection Using Deep Learning in the SCADA System of Electric Vehicle Charging Station “Manoj Basnet Department of Electrical and Computer Engineering University of Memphis Memphis, TN, USA.

4.International Journal of Ripples, Multiresolution and Information Processing Optimized deep piled autoencoder for ransomware discovery using blockchain network Nalinipriya, Balajee Maram, Ch. Vidyadhari andR. Cristin.

5.Ransomware detection using deep learning based unsupervised feature extraction and a cost sensitive Pareto Ensemble classifier Umme Zahoora1, Asifullah Khan1,2,3*, Muttukrishnan Rajarajan4*, Saddam Hussain Khan1,5, Muhammad Asam1 & Tauseef Jamal1

6. Narayanan Balkrishnan and Dr. Govindarajan Muthukumarasamy. Crop production Ensemble

Machine Learning model for prediction. The 11th ACM International Conference on Management of Digital EcoSystems (2019)

7. Kolter, J.Z.; Maloof, M.A. Learning to descry and separate vicious executables in the wild.J. Mach. get.Res. 2006, 7, 2721 – 2744.

8.Zakaria,W.Z.A.;Mohd,M.F.A.O.;Ariffin,A.F.M. The advancement of Ransomware. In suits of the 2017 International Conference on Software ande-Business, ICSEB 2017, Hong Kong, 28 – 30 December 2017;pp. 66 – 70