Tennessee TECH

Deep Learning Based Malware Classification in Cloud IaaS

Austin Brown[1] , Phillip Brown[1] , Andrew McDole[1] , Maanak Gupta[1] , and Mahmoud Abdelsalam[2]
[1]Tennessee Technological University, Cookeville, TN, USA
[2]Manhattan College, Riverdale, NY, USA

BACKGROUND

Cloud infrastructure has presented great opportunities for consumers to harness virtualized computing power on demand, but it also present a major attack vector for attackers.

Because of this, constant monitoring of assets is essential for datacenters to protect their customers data and privacy. One solution to this monitoring is machine learning or more specifically, deep learning which is usually in the form of neural networks which imitate brain structure to learn.

STATIC ANALYSIS

In static malware analysis, files are scanned for malicious content before they are executed on a system. Once a program is deemed to be benign, it is allowed to execute normally without further monitoring. This approach often fails in cloud infrastructures where attackers can inject malware into existing applications which are already deemed to be safe and not subject to rescanning.

DYNAMIC ANALYSIS

Dynamic Analysis, as opposed to static analysis, attempts to analyze already running applications for signs of malicious activity. Certain metrics from a running virtual machine and its processes can be used to categorize that virtual machine as being infected with malware or running normally.

A neural network can take in this metric information and learn how to predict when a virtual machine is infected or not.

By combining machine learning and dynamic analysis techniques, accurate identification of malware infected virtual machines can be achieved

PREVIOUS WORK

Initial work has been conducted in this area [1][3]. This paper delivers a methodology to extract and format information from virtual machines in a cloud infrastructure and format this information for processing in a 2-Dimensional Convolutional Neural Network (2D CNN).

$$
\mathbf{X}_t = \begin{array}{c|cccc|}
 & f_1 & f_2 & \cdots & f_n \\
p_1 & \vdots & \vdots & \cdots & \vdots \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
p_m & \vdots & \vdots & \cdots & \vdots
\end{array}
$$

2D matrix of features and processes for input into a 2D CNN [4]

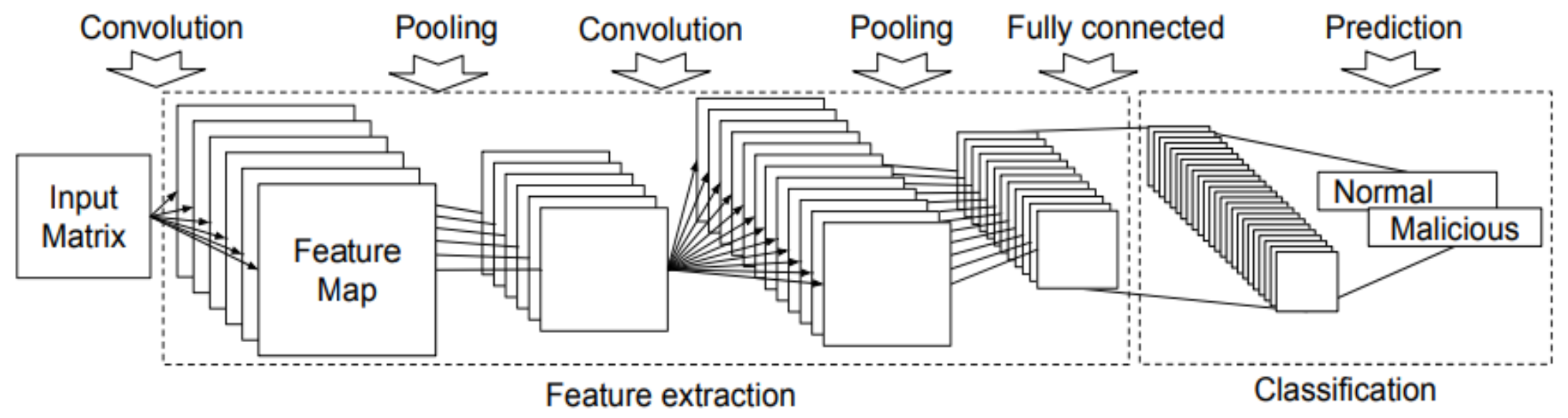
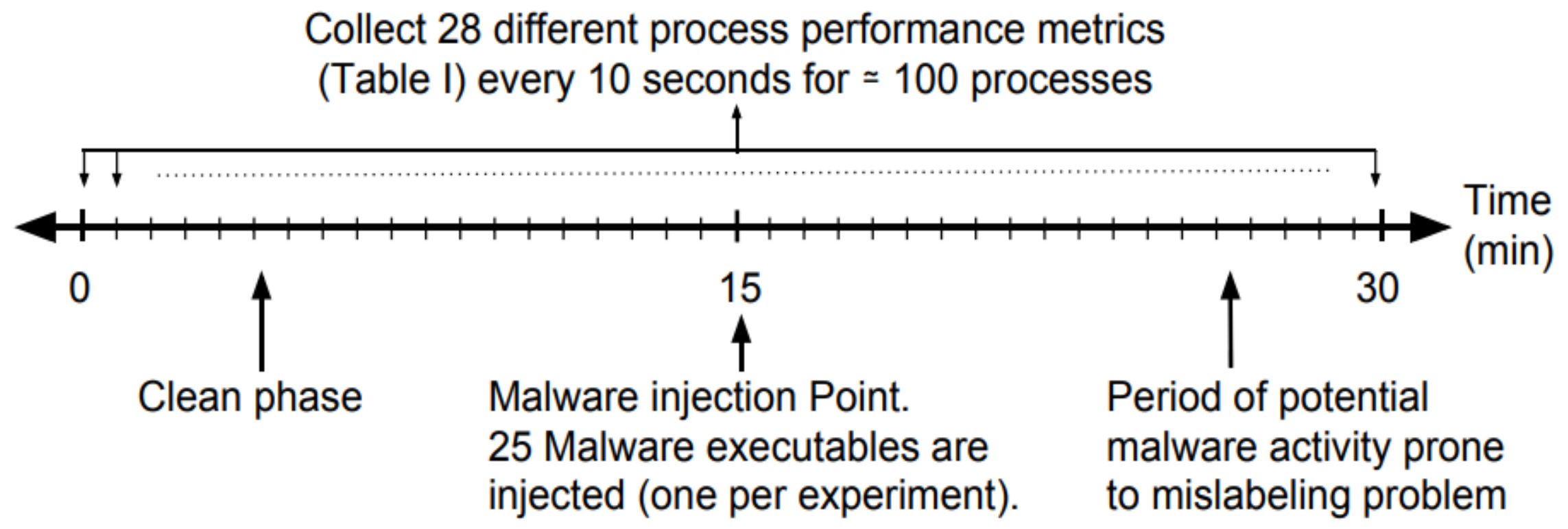


Diagram of a 2D CNN [4]

[1] used Openstack [2] to virtualize a 3-tier web architecture and simulated web requests using a multi-process traffic generator. Experiments were 30 minutes long where a single malware was injected into one virtual machine after 15 minutes. Results were collected every 10-seconds.


Collect 28 different process performance metrics (Table I) every 10 seconds for ≈ 100 processes
Time (min)
0
15
30
Clean phase
Malware injection Point. 25 Malware executables are injected (one per experiment).
Period of potential malware activity prone to mislabeling problem

Data Collection Overview [4]

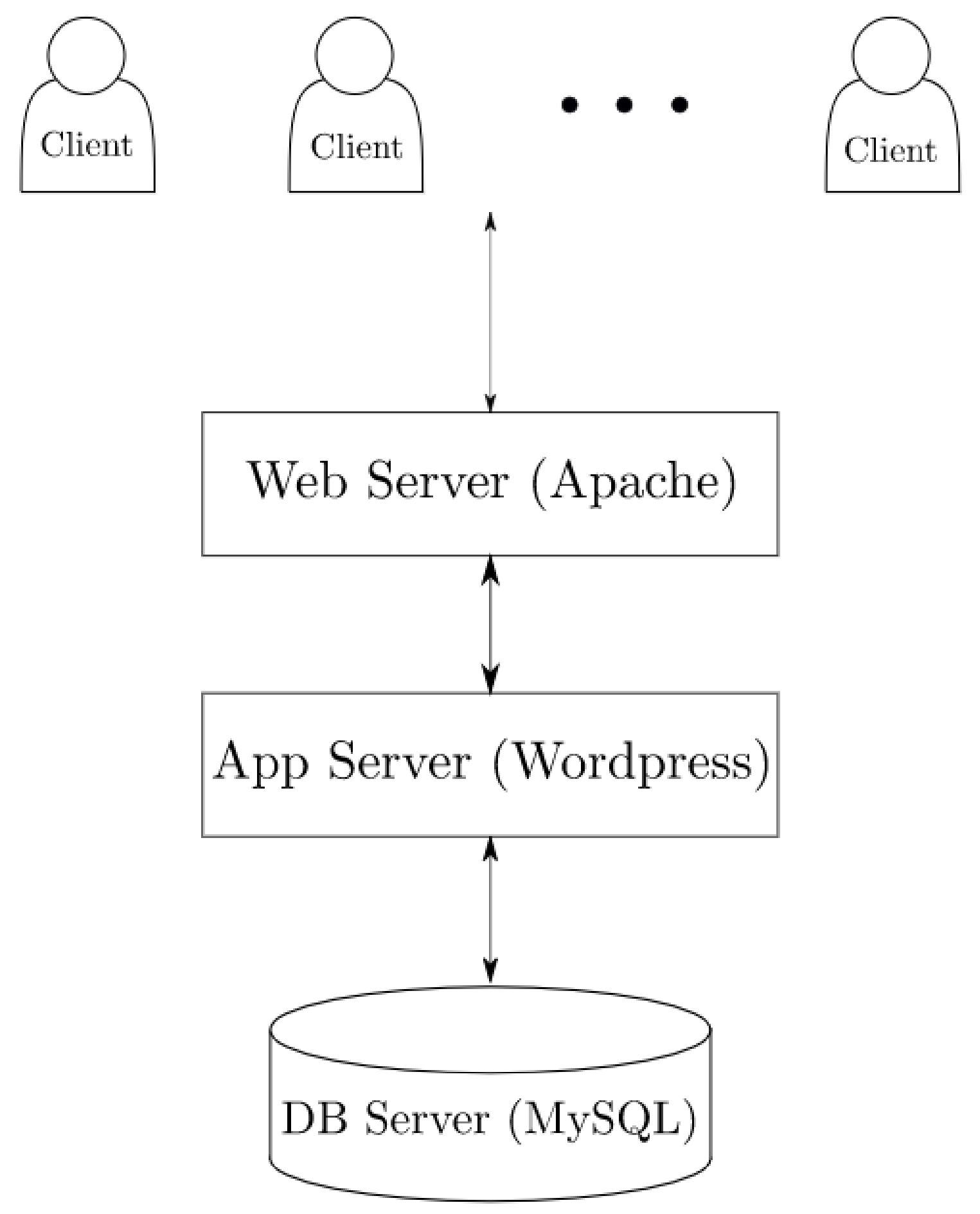
This model resulted in a ~75% accuracy when tested with different batch sizes. A 3-dimensional CNN has been used [1] to increase the accuracy to ~97%.

OUR RESEARCH

Our research focuses on malware classification rather than malware detection. Our research goals include the generation of malicious data and the use of that data in malware classification in cloud environments.

Setup

Our research utilizes and OpenStack testbed. This test bed is designed to represent a near-real cloud environment through setting up virtual machines in typical cloud architectures. Below represents a possible 3-tier web architecture setup common in cloud IaaS environments.



Data Generation

We used 6073 malicious binaries designed for Windows. The experimental period lasted 20 minutes and consisted of a 10-minute benign phase and a 10-minute malicious phase. During the benign phase, the VM operated normally with no infection. We collected samples every 10 seconds using metrics gathered from the performance counters built into Windows. Each VM became infected with malware at the 10-minute mark in the experiment with a unique malware from the 6073 malwares.

Malware Classification

While our previous work dealt with malware detection, we are working on malware classification. Malware classification is more complex than malware detection for our data. While malware detection is a binary prediction, malware classification is as complex as the number of classes of malware. Our 6073 malware binaries belong to 13 classes of malware plus the benign class. We are performing a comparative analysis of various classical machine learning techniques and deep learning techniques for the purpose of malware classification using our cloud data.

Future Work

We are exploring alternative cloud environments to generate data in. Currently we plan to work with containerized environments as containers are widely used in industry cloud environments. We are also continually tuning and working on our malware classification performance with our machine learning models.

References

[1] M. Abdelsalem, R. Krishnan, and Y. Huang, "Malware Detection in Cloud Infrastructures using Convolutional Neural Networks," in *Proc. of the 2018 IEEE 11th International Conference on Cloud Computing, July 2-7 2018, San Francisco, CA* [Online]. Available: IEEE Xplore, http://www.ieee.org. [Accessed: Nov. 27 2019].

[2] D. Deloche, *Unfolded basic recurrent neural network [Online Image].* Available: Wikipedia.org, [Accessed: Nov. 27 2019]

[3] Abdelsalam M., Krishnan R., Sandhu R. (2019) *Online Malware Detection in Cloud Auto-scaling Systems Using Shallow Convolutional Neural Networks.* In: *Foley S. (eds) Data and Applications Security and Privacy XXXIII. DBSec 2019*. Lecture Notes in Computer Science, vol 11559. Springer, Cham

Cybersecurity Education, Research & Outreach Center
TENNESSEE TECH

Tennessee Technological University

Computer Science
TENNESSEE TECH