

# ERIC NUNES

1215 E. Lemon Street, Apt #105, Tempe, AZ-85281

Website: <https://efnunes.github.io/>

Email: [enunes1@asu.edu](mailto:enunes1@asu.edu)

Contact: 315-439-3089

## SUMMARY

Computer Engineering Graduate student with 4 years' experience in research and development of data analysis tools. Hands-on experience with Python, R, SQL, C++, and MATLAB. Knowledgeable in processes and tools related to Big Data and Data Science.

## EDUCATION

### PhD in Computer Engineering

Arizona State University, AZ

GPA: 4.0

Present

### Master of Science in Electrical Engineering

Syracuse University, NY

May, 2012

### Bachelor of Science in Electronics and Telecommunication

University of Mumbai, India

June, 2010

## TECHNICAL SKILLS

- **Machine Learning:** Classification, regression, clustering, anomaly detection, feature engineering, online learning, Experience with deep learning.
- **Programming Languages:** Python, MATLAB, C++, Prolog, HTML, and LaTeX. Familiar with C, R.
- **Libraries:** scikit-learn, Elasticsearch, Weka, Pandas, Theano, Caffe.
- **Databases:** SQL, PostgreSQL, MongoDB.
- **Big Data and Cloud:** Splunk, Spark, Familiar with Big Data Processing Platforms: Hadoop and Cloud tools: Amazon S3.

## KEY PROFESSIONAL AND RESEARCH EXPERIENCE

### Data Scientist / Researcher, Cyber Reconnaissance Inc. (CYR3CON)

June 2016 - Present

Tools: Python, PostgreSQL, MongoDB, Spark.

- Designed a system to store and mine data from darknet markets and forums.
- Leading a team of developers and analysts to build tools/products for security applications. In particular,
  - Leveraging threat intelligence to build learning models for predicting likelihood of exploitation of a vulnerability (vulnerability prioritization),
  - Providing intelligence on Mobile threats (both Android and iOS applications),
  - Active threat assessment on client systems,
  - Named-entity recognition (to determine vulnerable software) using RNN/LSTM seq2seq models,
  - Building classification models to identify malicious web scripts (PHP/HTML).
  - Assist with the expansion of CYR3CON future product features as well as the management and development of growing community of users, guiding/assisting them in trials and integrating with client systems.

### Security Automation Intern (Data Science), PayPal

May 2017- August 2017

Tools: Python, Splunk, Spark.

- Analyzed user login activity using Akamai logs and enriched it with other data feeds such as threat intelligence, merchant data, credential dumps.
- Implemented operational Anomaly detection models to detect Account Takeover (ATO) attacks to raise alerts.
- Visualized ATO attacks in real time on a dashboard in Splunk to aid risk to flag fraudulent transactions.

### Graduate Research Assistant, CySIS Lab, Arizona State University

August 2014 - Present

Tools: Python, PostgreSQL, Prolog, tcpflow.

- Modeling of threat actors: Identifying cyber adversaries using argumentation and machine learning models (knowledge base: 10 million attacks).
- Proactive Cyber-Threat Intelligence: Built a system to crawl and parse the Darknet (markets and forums) to extract cyber threat intelligence including zero-day exploits using data mining and machine learning techniques. Identifying targeted software through disclosed vulnerabilities on Darkweb.
- Malware task identification: Identifying the tasks that a piece of malware was designed to perform on the system (adversarial intent) using cognitive learning models.

## PATENTS

- Systems and Methods for predicting which software vulnerabilities will be exploited by malicious hackers to prioritize for Patching, Submitted, 2017.
- Systems and Methods for Data Driven Malware Task Identification. Submitted, 2016.
- Intelligent darkweb crawling infrastructure for cyber threat intelligence collection. Licensed to CYR3CON, 2016.

## REFERRED PUBLICATIONS

<https://efnunes.github.io/publication.html>