Machine Learning in Cyber Security

Shawn Saliyev

Division of Science and Mathematics
University of Minnesota, Morris
Morris, Minnesota, USA

17 November 2018
UMM, Morris

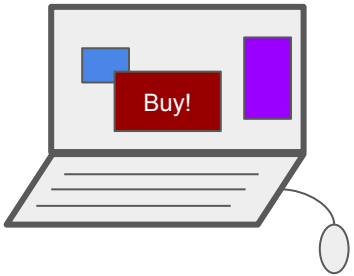
What is Malware

Malicious Software

What is Malware

Malicious Software

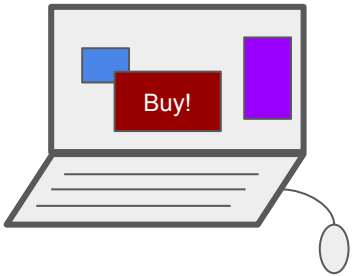
Adware



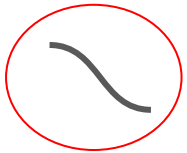
What is Malware

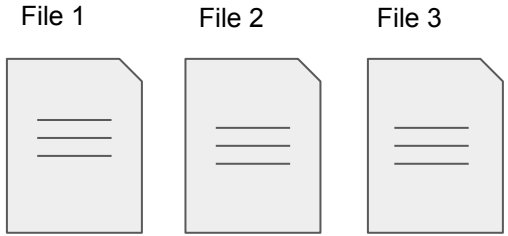
Malicious Software

Adware



Worm

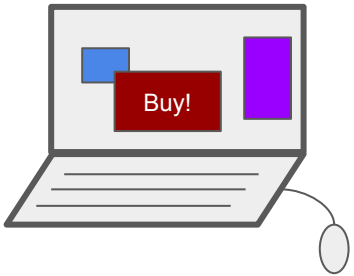




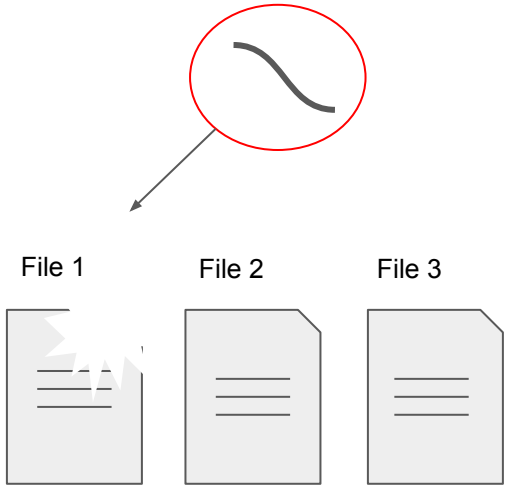
What is Malware

Malicious Software

Adware



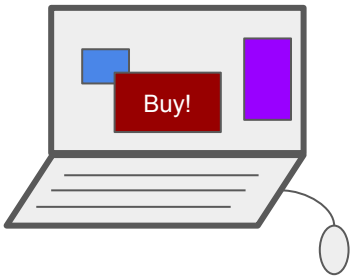
Worm



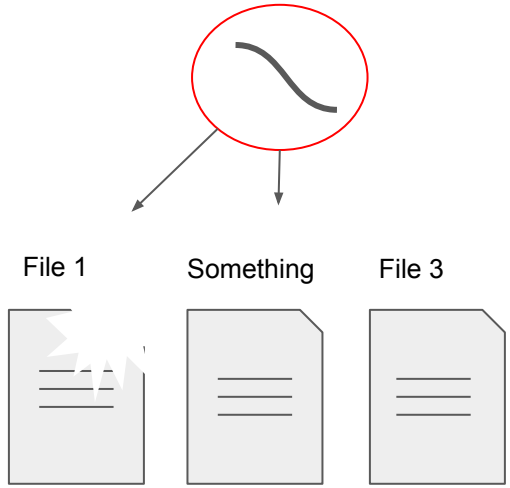
What is Malware

Malicious Software

Adware



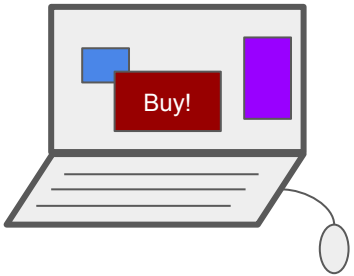
Worm



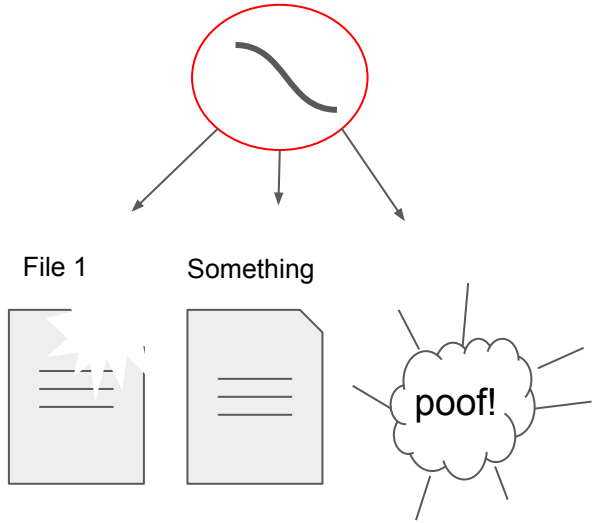
What is Malware

Malicious Software

Adware



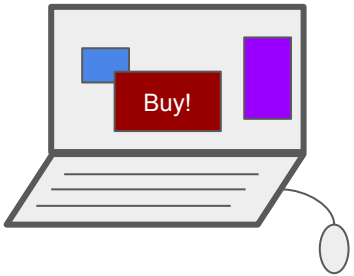
Worm



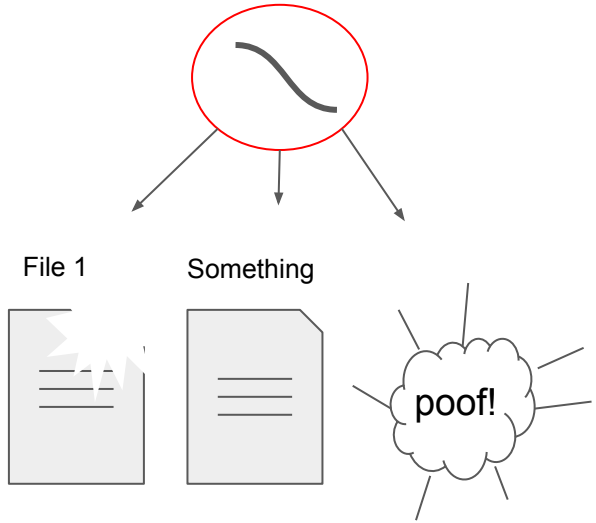
What is Malware

Malicious Software

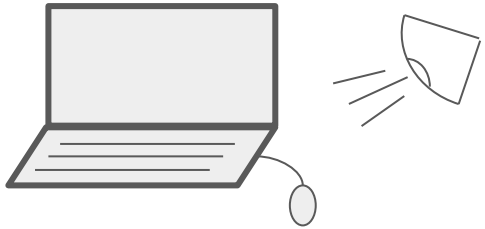
Adware



Worm



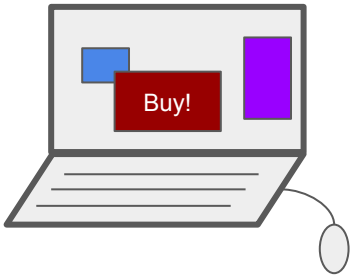
Spyware



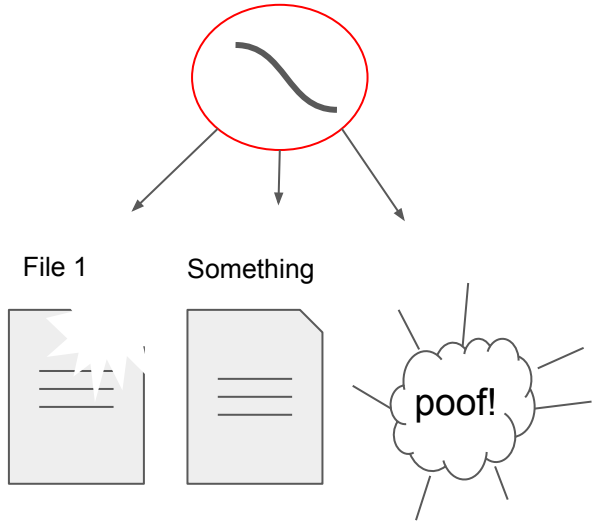
What is Malware

Malicious Software

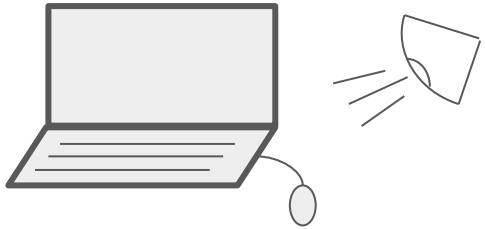
Adware



Worm



Spyware



- KeyLogger

Why use Machine Learning for Detecting Malware?

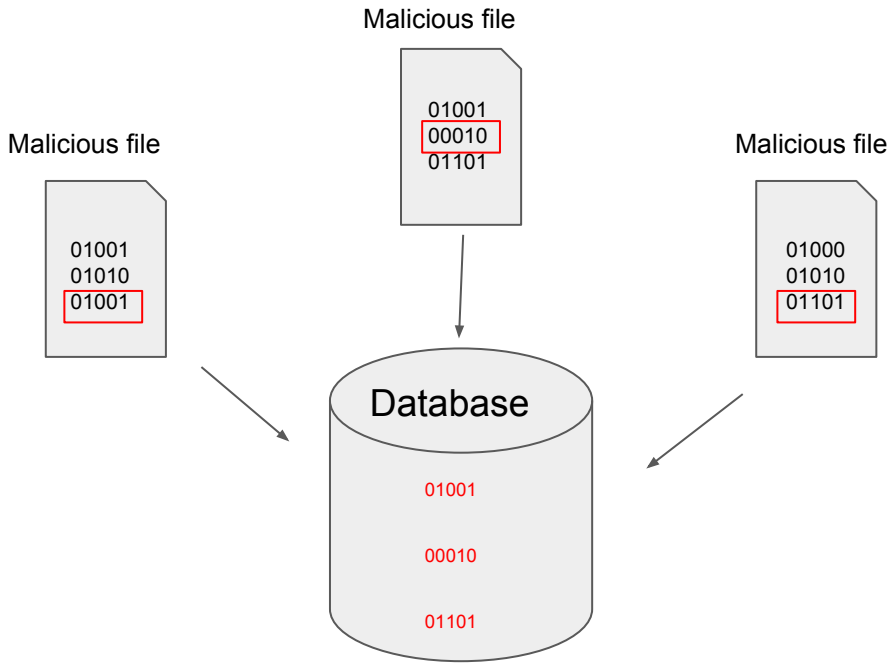
- Dynamic Environment
- More Advanced types of Malware
- New Efficient Detection Systems

Old Traditional Way for Detecting Malware

Signature Based Detection System

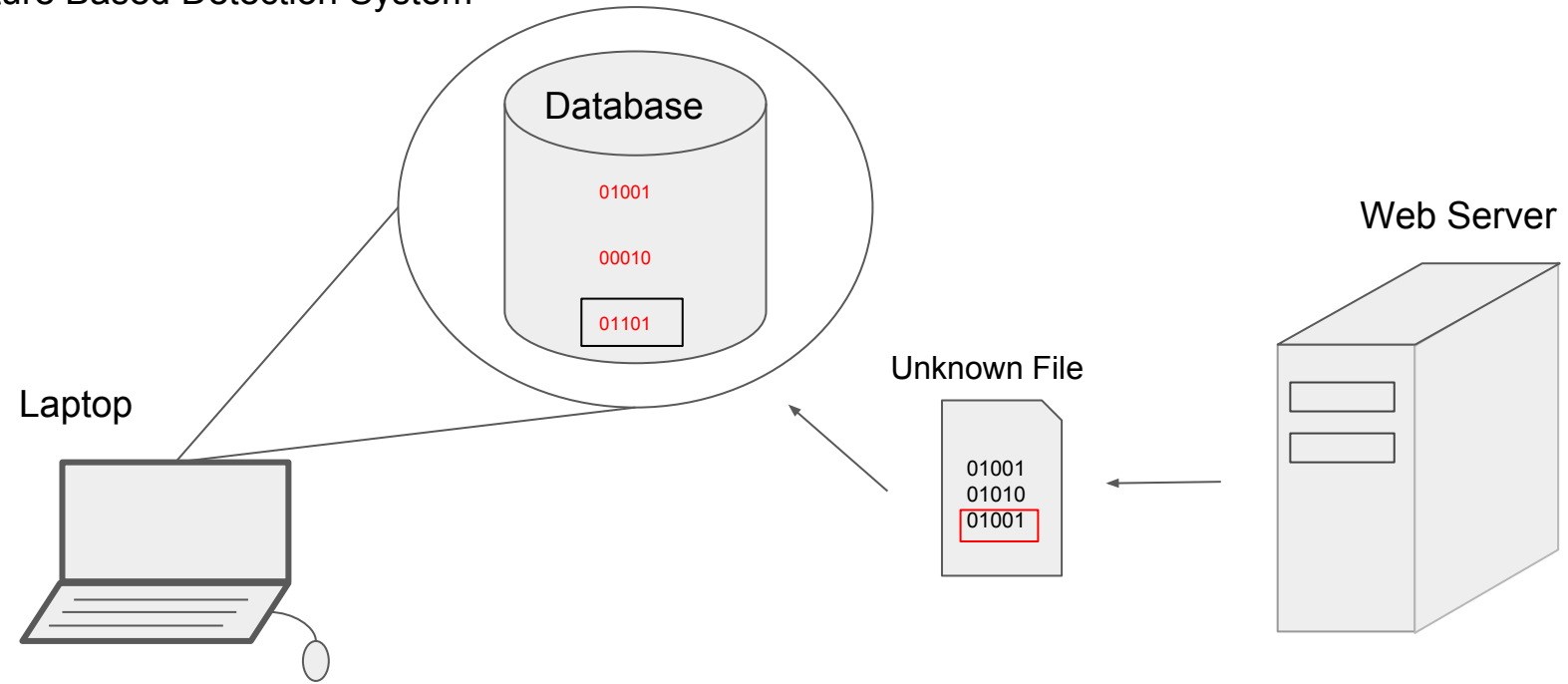
Signature

- Instruction Sequences
- Binary Sequences



Old Traditional Way for Detecting Malware

Signature Based Detection System



Old Traditional Way for Detecting Malware

Signature Based Detection System

Weaknesses

- Zero Day Attacks
- Polymorphic Malwares

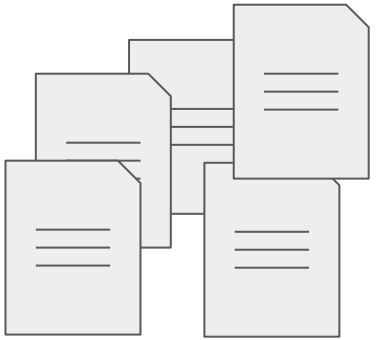
Outline

- Background
  - Machine Learning
  - Deep Neural Network
- Deep Neural Network Approach
  - Data Gathering
  - Structure Data Generation
  - Feature Extraction
  - Modeling
  - Results
- Conclusion

Background

Machine Learning

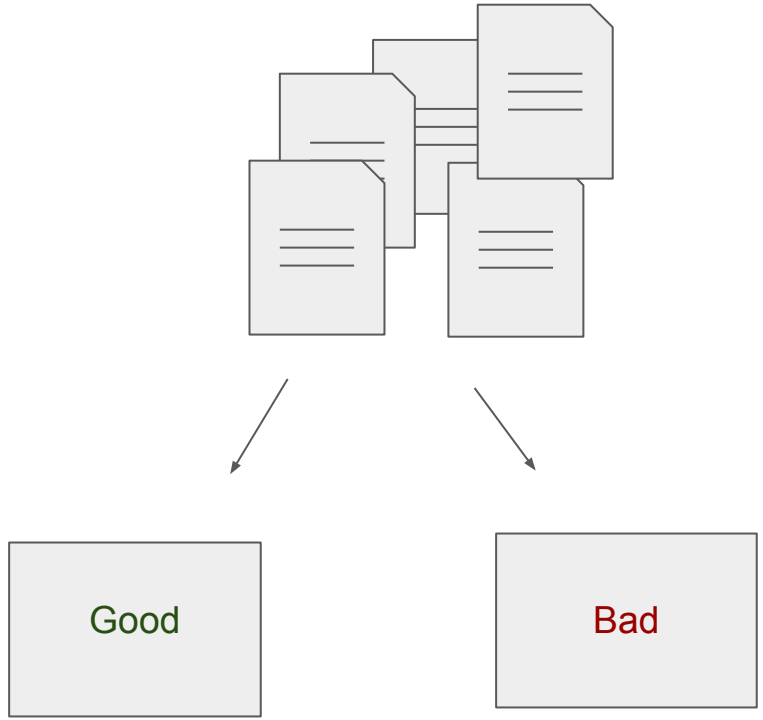
- Process Big Multidimensional Data



Background

Machine Learning

- Process Big Multidimensional Data
- Categorization of Data



Background

Machine Learning

- Supervised
  - Labeled Data
  - Classification

Background

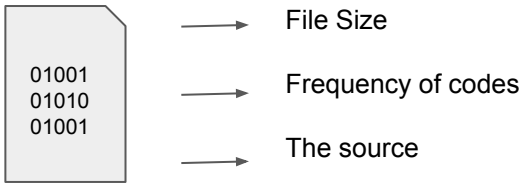
Machine Learning

- Supervised
  - Labeled Data
  - Classification
- Unsupervised
  - Unlabeled Data
  - Clustering

Background

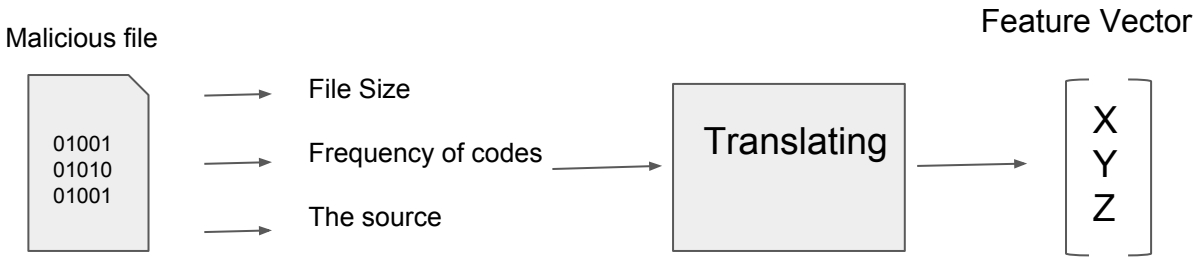
Machine Learning

Malicious file



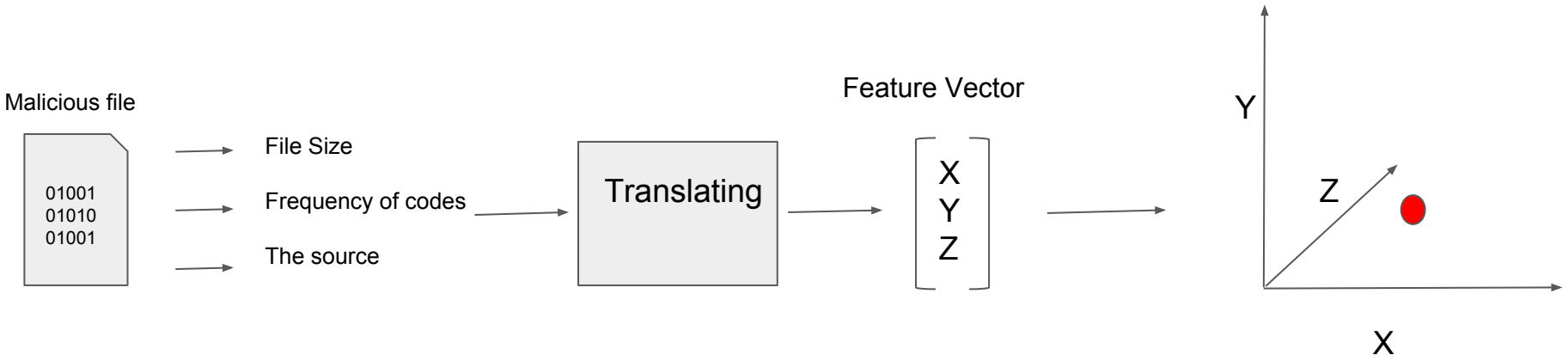
Background

Machine Learning



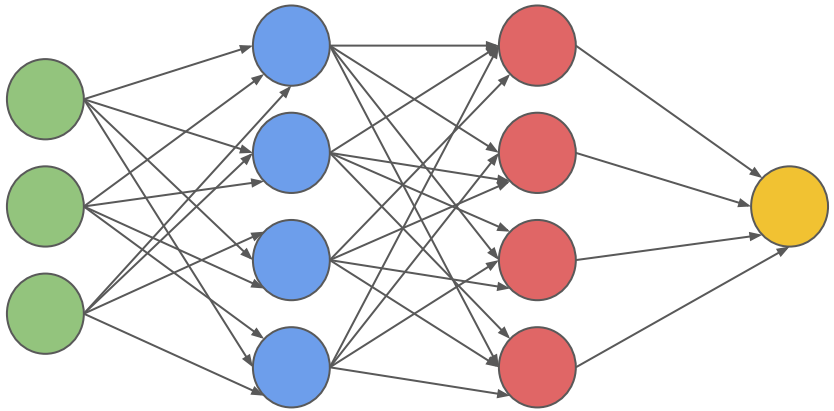
Background

Machine Learning



Background

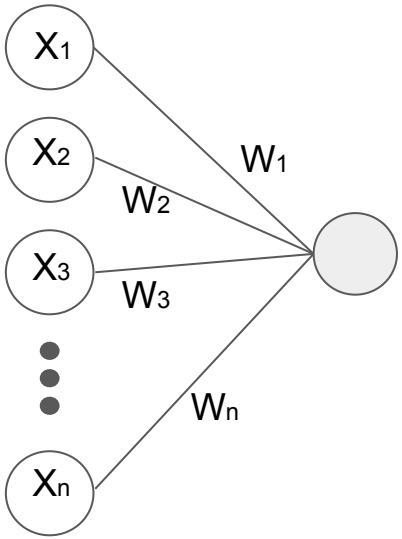
Deep Neural Network



Input layer Hidden layer 1 Hidden Layer 2 Output Layer

Background

Deep Neural Network



Activation Function ($W_1 * X_1 + W_2 * X_2 + W_3 * X_3 + .. + W_n * X_n$)

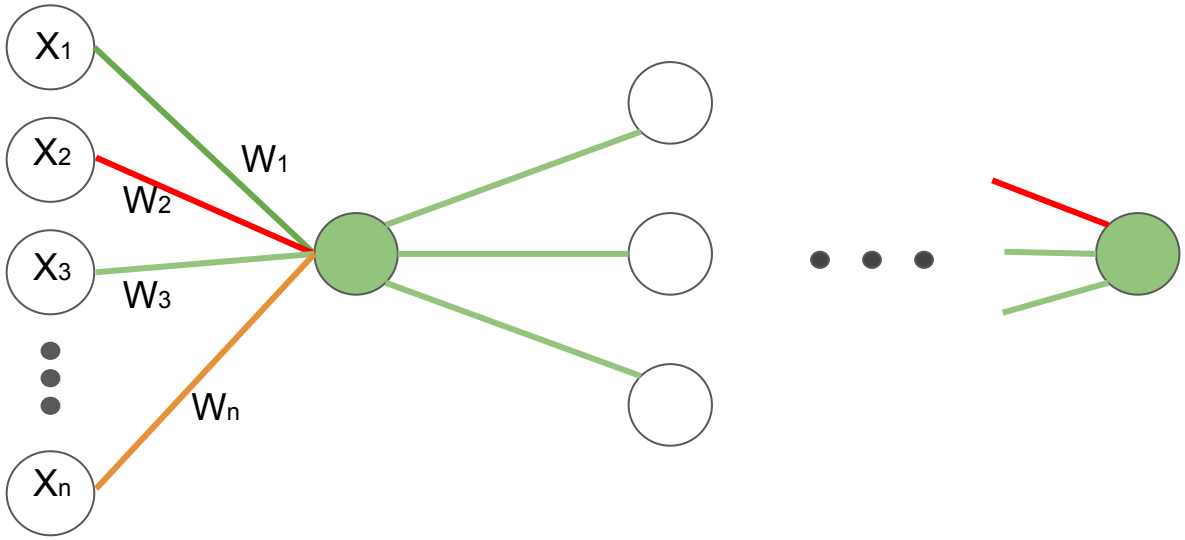
Example
Activation Function - ELU

$$f(x) = \begin{cases} x & if\ x \geq 0 \\ a(e^x - 1) & if\ x < 0 \end{cases}$$

Input Layer Hidden Layer

Background

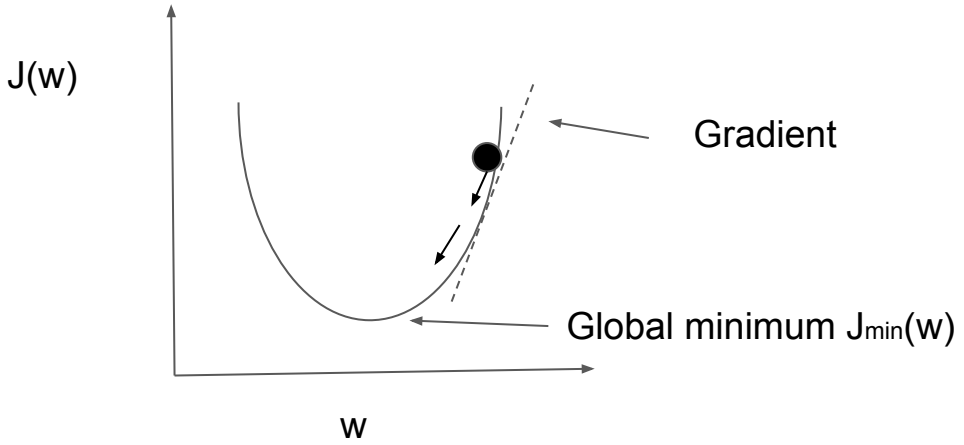
Deep Neural Network



Background

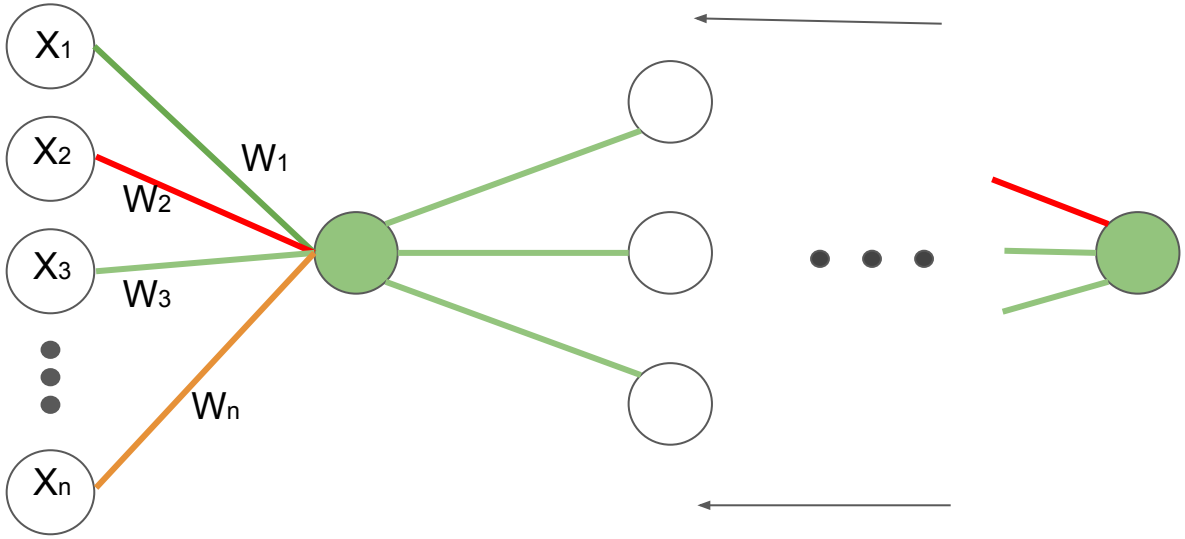
Deep Neural Network

- Loss Function - J(w)
- Back Propagation



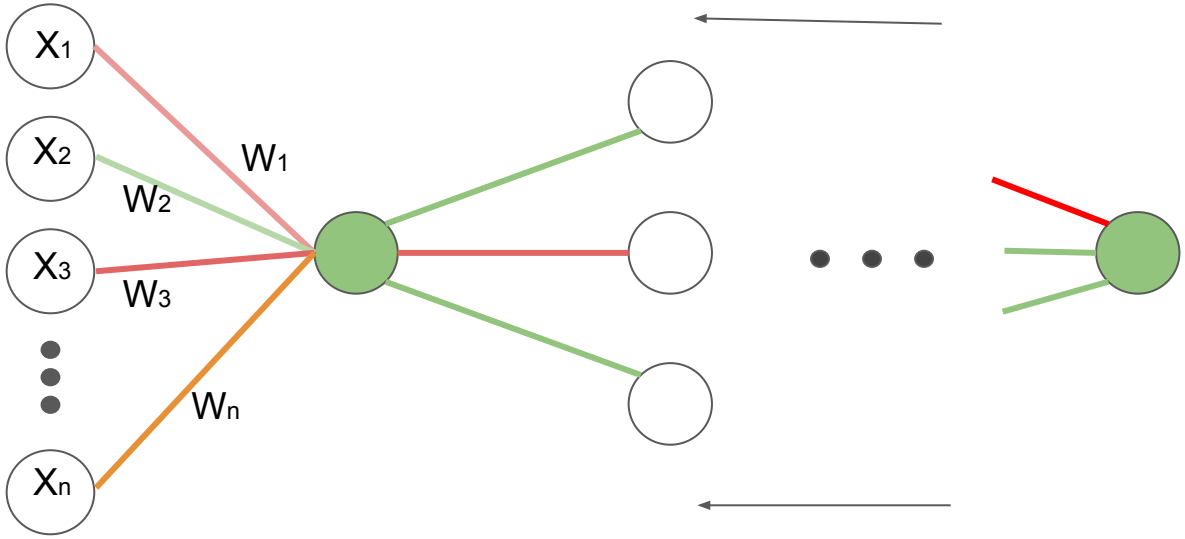
Background cont.

Back Propogation



Background cont.

Back Propagation



Outline

- Background
  - Machine Learning
  - Deep Neural Network
- Deep Neural Network Approach

Deep Neural Network Approach

Data Gathering

Deep Neural Network Approach

Data Gathering

- Malicious Files
  - Malicia Project
  - 11,064 Assembly Files

Deep Neural Network Approach

Data Gathering

- Malicious Files
  - Malicia Project
  - 11,064 Assembly Files
- Benign Files
  - Windows Systems
  - 2,800 Assembly Files
  - Adaptive Synthetic oversampling technique (ADASYN)

Deep Neural Network Approach

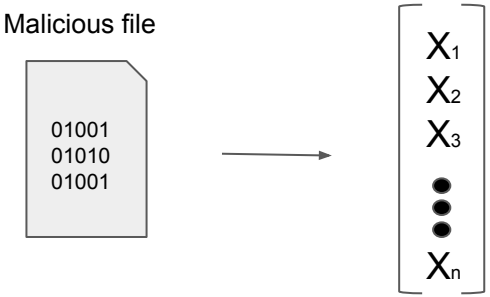
Data Gathering

- Malicious Files
  - Malicia Project
  - 11,064 Assembly Files
- Benign Files
  - Windows Systems
  - 2,800 Assembly Files
  - Adaptive Synthetic oversampling technique (ADASYN)
- Total around 22,000 Assembly Files
  - ~ 15,000 Files for Training
  - ~ 7,000 Files for Testing

Deep Neural Network Approach cont.

Structure Data Generating

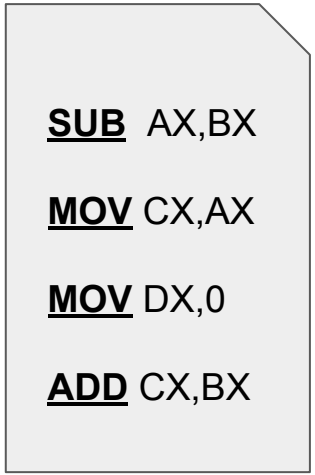
- Opcode
- Frequency Tables



Deep Neural Network Approach cont.

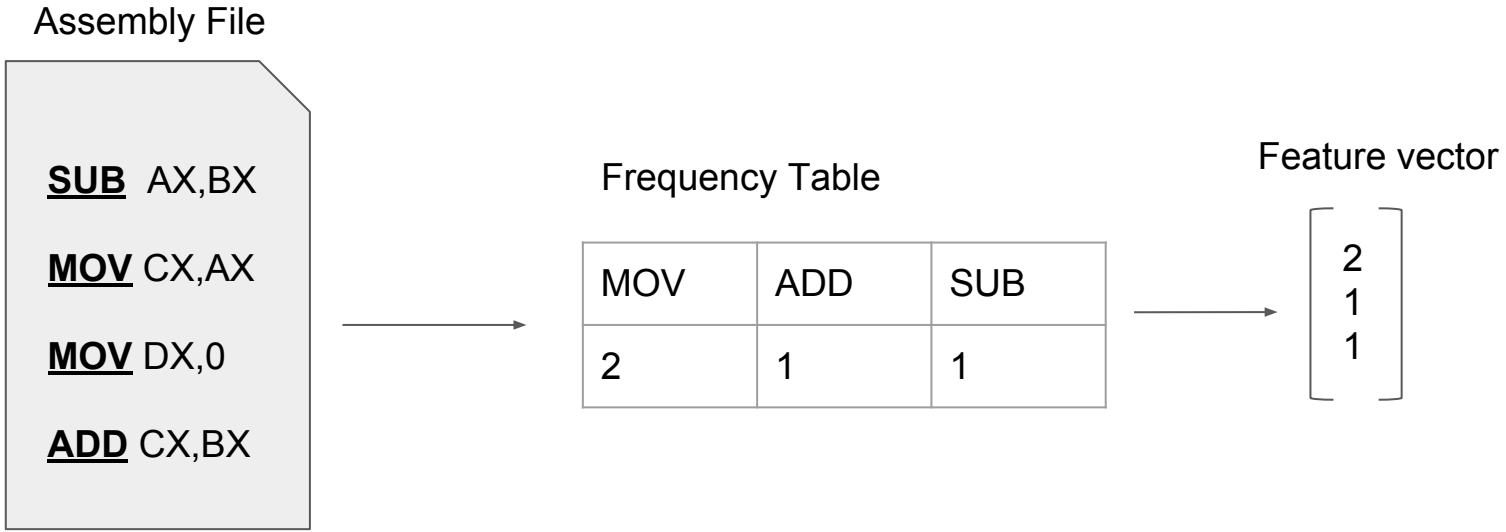
Operation Code (Opcode)

Assembly File



Deep Neural Network Approach cont.

Generating Frequency Table

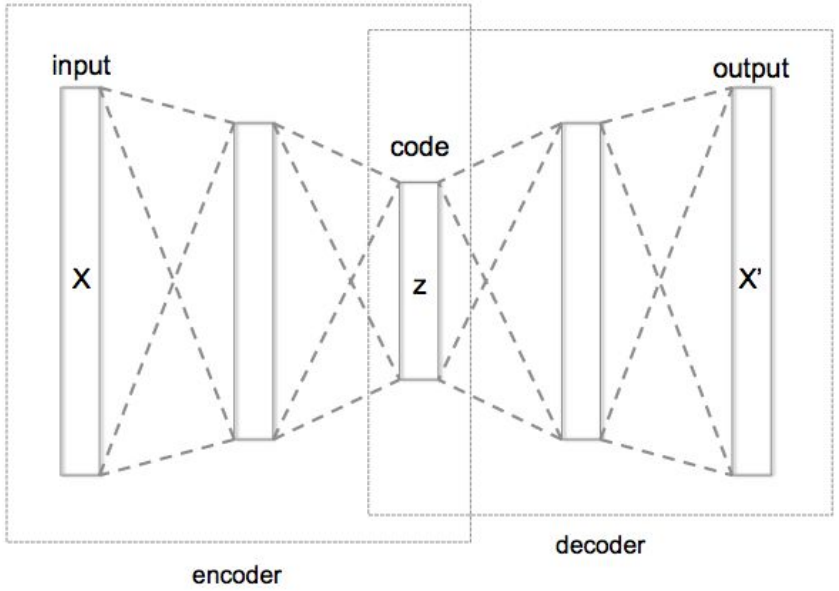


Deep Neural Network Approach cont.

Feature Extraction

Autoencoder (AE)

- Encoder
- Decoder
- Bottleneck Layer

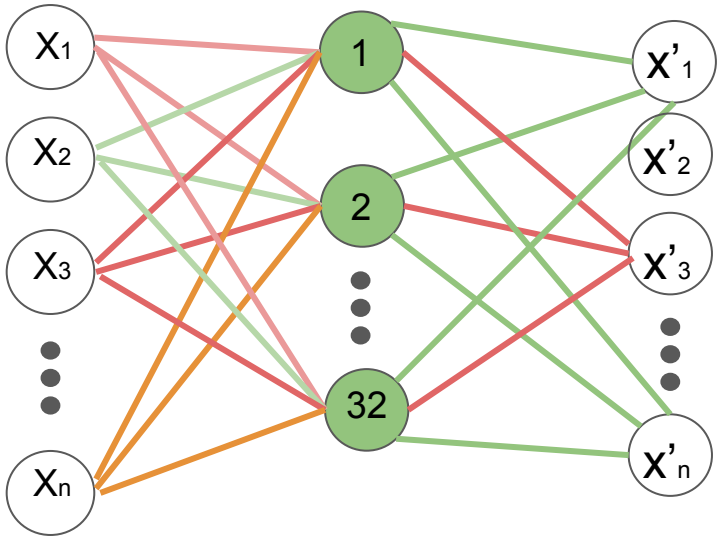


Deep Neural Network Approach cont.

Feature Extraction

Autoencoder (AE)

- 1-Layer Autoencoder

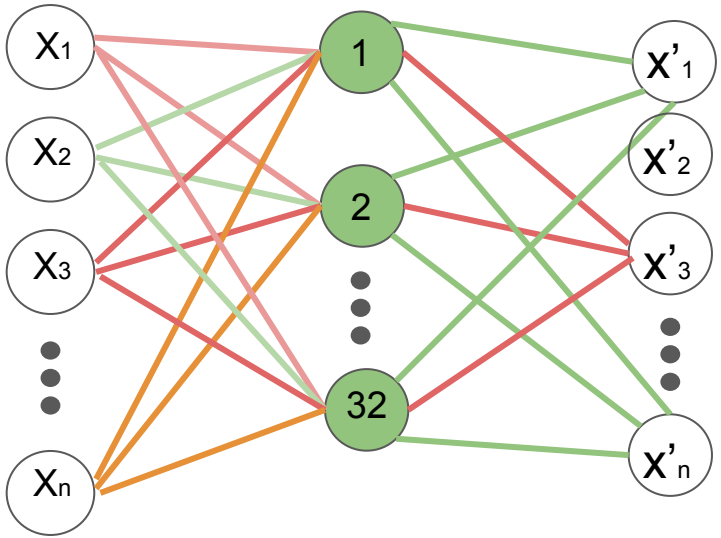


Deep Neural Network Approach cont.

Feature Extraction

Autoencoder (AE)

- 1-Layer Autoencoder
- 3-Layer Autoencoder

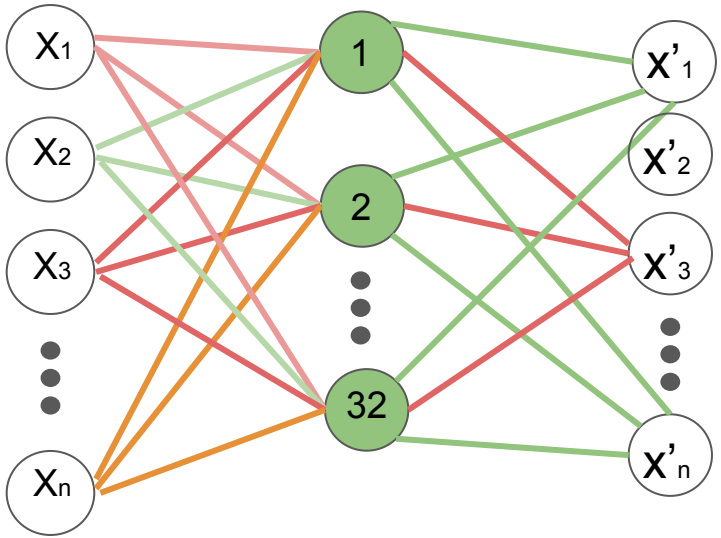


Deep Neural Network Approach cont.

Feature Extraction

Autoencoder (AE)

- 1-Layer Autoencoder
- 3-Layer Autoencoder
- ADAM optimizer

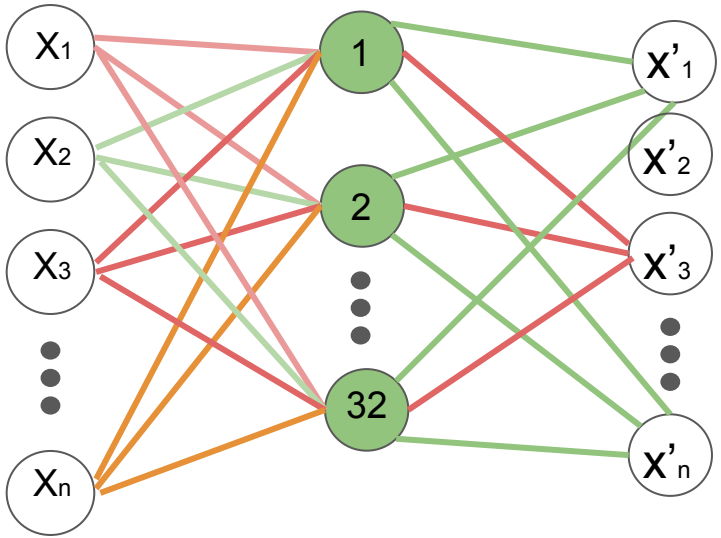


Deep Neural Network Approach cont.

Feature Extraction

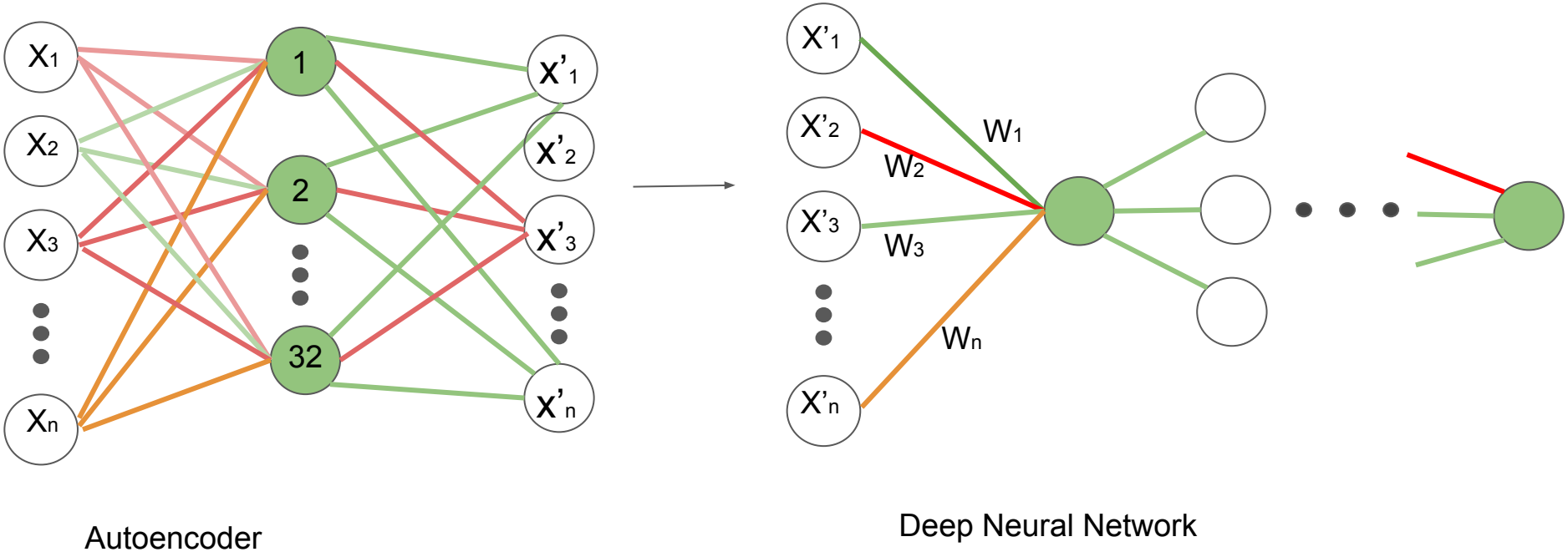
Autoencoder (AE)

- 1-Layer Autoencoder
- 3-Layer Autoencoder
- ADAM optimizer
- ELU Activation Function



Deep Neural Network Approach cont.

Modeling



Autoencoder

Deep Neural Network

Deep Neural Network Approach cont.

Modeling

Deep Neural Network

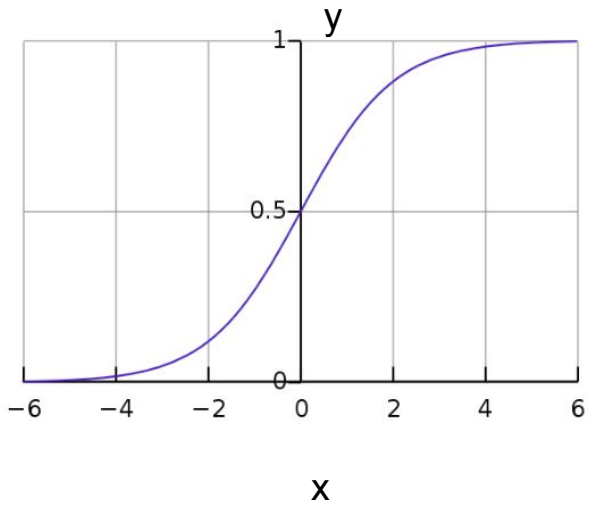
- 2-hidden layer DNN
- 4-hidden layer DNN
- 7-hidden layer DNN
- ELU (Activation Function)
- Output Layer - Sigmoid Activation
- ADAM optimizer

Deep Neural Network Approach cont.

Modeling

Deep Neural Network

- 2-hidden layer DNN
- 4-hidden layer DNN
- 7-hidden layer DNN
- ELU (Activation Function)
- Output Layer - Sigmoid Activation
- ADAM optimizer



Deep Neural Network Approach cont

Results

Outline

- Background
  - Machine Learning
  - Deep Neural Network
- Deep Neural Network Approach
  - Data Gathering
  - Structure Data Generation
  - Feature Extraction
  - Modeling
  - Results
- Conclusion

Conclusion

- Cyber Security is really important
- Deep Neural Network shows good performance
- There are still more techniques to explore

Acknowledgements

Thank you for your time and attention!

Special thanks to K.K. Lamberty, Elena Machkasova and Nic McPhee for your guidance and feedback.

References

- Mohit Sewak, Sanjay K. Sahay, and Hemant Rathore. 2018. An investigation of a deep learning based malware detection system. In Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES 2018). ACM, New York, NY, USA
- I. Goodfellow, Y. Bengio, and A. Courville.DeepLearning. MIT Press, 2016. http://www.deeplearningbook.org
- Wikipedia contributors. (2018, November 13). Malware. In *Wikipedia, The Free Encyclopedia*. Retrieved 11:36, November 18, 2018, from https://en.wikipedia.org/w/index.php?title=Malware&oldid=868580417
- Wikipedia contributors. (2018, November 3). Intrusion detection system. In *Wikipedia, The Free Encyclopedia*. Retrieved 11:37, November 18, 2018, from https://en.wikipedia.org/w/index.php?title=Intrusion_detection_system&oldid=867076009