Prevention of Attacks using One-Class Classification and Autoencoders

By

18BCI0247 Rohan Allen

18BCI0109 Rakshith Sachdev

18BCI0192 Harshita Pundir

Under the Guidance of

Dr. Swarnalatha. P

School of Computer Science and Engineering

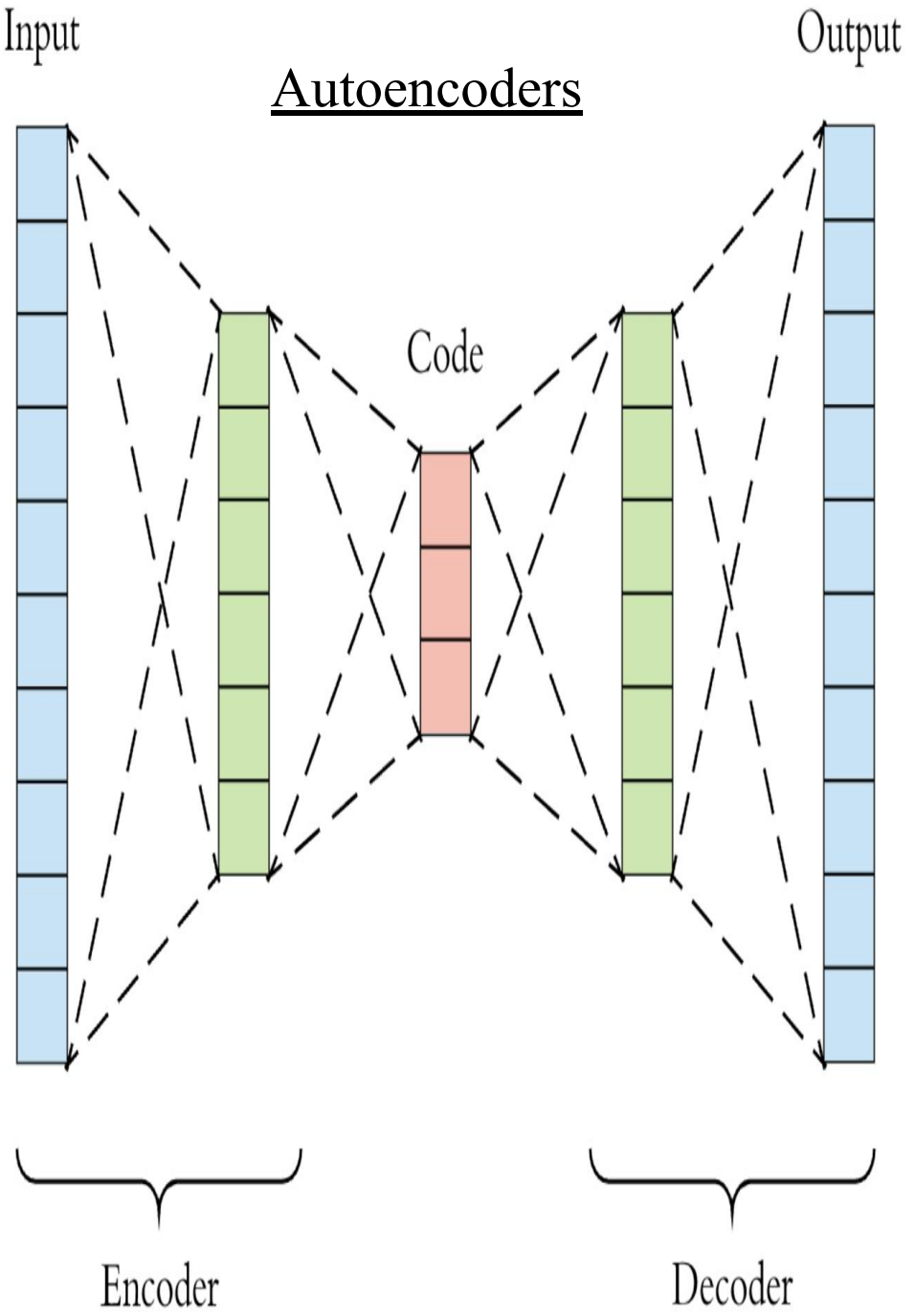
Disaster Recovery and Business Continuity Management BCI3002-Fall 2021

VIT®

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Autoencoders



OUTLINE

- AIM AND SCOPE
- ABSTRACT/PROBLEM STATEMENT
- OBJECTIVES (GAPS IDENTIFIED)
- SCHEDULE DIAGRAM OF THE SYSTEM
- BLOCK DIAGRAM OF THE SYSTEM/ARCHITECTURE OF THE SYSTEM
- SOLUTION FOR THE OBJECTIVES AND METRICS APPLIED
- RESULTS AND DISCUSSION WITH GRAPHS
- *Implementation – [Demo]*- Video Recorded File

(include uniqueness out of project in terms of graph)

- GLOSSARY
- CONCLUSION
- REFERENCES (MINIMUM 10 REFERENCES)

AIM AND SCOPE

- AIM AND SCOPE

The aim of this project is to train our system to differentiate between bad network traffic which might contain some virus, malware to the system, or any other type and normal network using machine learning and to perform DRBCM process on it. The model has also been trained to predict false data and henceforth prevent the installation of any particular software during the risk of an attack, which results in an increased cost. The main key objective is to provide maximum accurate results by using / one class-based modeling approach and reducing the processing time significantly.

ABSTRACT/PROBLEM STATEMENT

- AIM AND SCOPE
- ABSTRACT/PROBLEM STATEMENT

With today's day and age rapidly becoming digital, the network and endpoint devices become a target for attacks and exploitation; thus, the systems have long been associated with issues related to security. Therefore, making systems secure and safe is of extreme importance. As per the 2020 Unit 42 Threat Report, practically all traffic is decoded, implying that the majority of classified and individual user information in the network is highly powerless against cyber attacks. Network security is utilized to delay unintentional harm which can be done to the network's private information, its users, or its devices. The main aim of network security is to secure the network running and for every single authentic client.

In this project, we represent how one-class classifiers are prepared to utilize generous information to recognize ordinary and dangerous traffic redirected to an endpoint device. In this venture, the framework is prepared to utilize unsupervised / one-class-based demonstrating approaches by which the framework would comprehend the issues that we would confront day by day, and the preparation will be useful for what's to come. After the preparation of the framework, the framework can be utilized in reality to confront ongoing, new difficulties and by gaining from the past experiences it can develop as indicated by the users' issues, weaknesses, dangers, and conditions

OBJECTIVES (GAPS IDENTIFIED)

- AIM AND SCOPE
- ABSTRACT/PROBLEM STATEMENT
- OBJECTIVES (GAPS IDENTIFIED)

The objective of this project is to use machine learning to teach our system to distinguish between malicious network traffic, which could contain a virus or malware, and regular network data. The model has also been taught to detect and avoid fake data and the deployment of any specific software while there is a threat of an attack, which results in dramatically reducing the financial stress on an organization and prevents tarnishing their reputation. The major goal is to offer the most accurate findings possible by utilizing methods such as unsupervised learning/one-class-based modeling, thereby lowering processing time substantially.

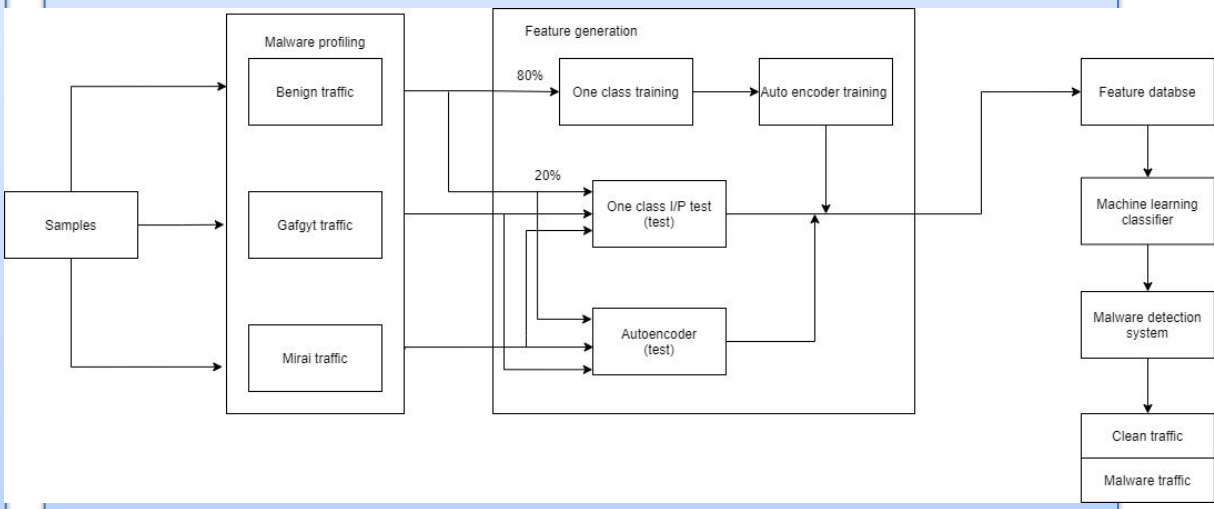
In this model, we are using one-class classifications and autoencoders so that the system can detect bad traffic more accurately. With the help of this model, we can predict false data, and therefore, we can prevent the installation of software at the time of any risks to decrease the cost.

SCHEDULE DIAGRAM OF THE SYSTEM

- AIM AND SCOPE
- ABSTRACT/PROBLEM STATEMENT
- OBJECTIVES (GAPS IDENTIFIED)
- SCHEDULE DIAGRAM OF THE SYSTEM

BLOCK DIAGRAM OF THE SYSTEM/ ARCHITECTURE OF THE SYSTEM

- AIM AND SCOPE
- ABSTRACT/PROBLEM STATEMENT
- OBJECTIVES (GAPS IDENTIFIED)
- SCHEDULE DIAGRAM OF THE SYSTEM
- BLOCK DIAGRAM OF THE SYSTEM/ARCHITECTURE OF THE SYSTEM



SOLUTION FOR THE OBJECTIVES AND METRICS APPLIED

- AIM AND SCOPE
- ABSTRACT/PROBLEM STATEMENT
- OBJECTIVES (GAPS IDENTIFIED)
- SCHEDULE DIAGRAM OF THE SYSTEM
- BLOCK DIAGRAM OF THE SYSTEM/ARCHITECTURE OF THE SYSTEM
- SOLUTION FOR THE OBJECTIVES AND METRICS APPLIED

MTD - This project can be divided into functionalities like malware profiling, feature generation, feature database, machine learning classifier, and finally malware detection which separates into malware traffic and clean traffic. Each functionality will have their own MTD based on their criticality. In this the machine learning classifier and malware detection are mission critical, and feature generation and feature database falls into business critical functionalities.

RTO - If any disaster occurs on this system, the response team begins the recovery process, which starts through the RTO process. This includes restoring backups of feature databases,and machine learning classifiers.

RPO - If any disaster occurs on this system, in the RPO phase, critical business functionality of the malware detection and traffic separation function is restored.

RESULTS AND DISCUSSION WITH GRAPHS

- AIM AND SCOPE
- ABSTRACT/PROBLEM STATEMENT
- OBJECTIVES (GAPS IDENTIFIED)
- SCHEDULE DIAGRAM OF THE SYSTEM
- BLOCK DIAGRAM OF THE SYSTEM/ARCHITECTURE OF THE SYSTEM
- SOLUTION FOR THE OBJECTIVES AND METRICS APPLIED
- RESULTS AND DISCUSSION WITH GRAPHS

Model Evaluation

ONE CLASS SVM MODEL EVALUATION

```
Confusion Matrix and Statistics

          Reference
Prediction  FALSE   TRUE
     FALSE 725065   2002
     TRUE       0   7907
```

AUTOENCODER IMPLEMENTATION

```
Confusion Matrix and Statistics

          Reference
Prediction  FALSE   TRUE
     FALSE 483435     20
     TRUE       0   4959
```

Implementation [Demo]-Video Recorded File

- AIM AND SCOPE
- ABSTRACT/PROBLEM STATEMENT
- OBJECTIVES (GAPS IDENTIFIED)
- SCHEDULE DIAGRAM OF THE SYSTEM
- BLOCK DIAGRAM OF THE SYSTEM/ARCHITECTURE OF THE SYSTEM
- SOLUTION FOR THE OBJECTIVES AND METRICS APPLIED
- RESULTS AND DISCUSSION WITH GRAPHS
- *Implementation – [Demo]-Video Recorded File*

Drive link for demo video:

https://drive.google.com/drive/folders/1QQ4b98J0qoIFA9gxD8PuaxD7Dhj0MHNI?usp=sharing

GLOSSARY

- AIM AND SCOPE
- ABSTRACT/PROBLEM STATEMENT
- OBJECTIVES (GAPS IDENTIFIED)
- SCHEDULE DIAGRAM OF THE SYSTEM
- BLOCK DIAGRAM OF THE SYSTEM/ARCHITECTURE OF THE SYSTEM
- SOLUTION FOR THE OBJECTIVES AND METRICS APPLIED
- RESULTS AND DISCUSSION WITH GRAPHS
- Implementation – Video Recorded File [Demo]
- GLOSSARY

ONE CLASS SVM: One-class SVM is an unsupervised algorithm that learns a decision work for curiosity identification: ordering new information as comparative or diverse to the preparation set. One-class classification algorithms are often used for binary classification tasks with a severely skewed class distribution. These techniques are used to fit on the input examples from the huge class within the training dataset, then evaluated on the remaining test dataset. Albeit not designed for these types of problems, one-class classification methods are frequently successful for unbalanced classification datasets with no or few instances of the minority class, or datasets with no cohesive structure to distinguish the classes that a supervised algorithm would learn. The SVM algorithm, which was originally designed for classification tasks, is frequently employed for one-class classification.

AUTOENCODERS: An autoencoder neural network is a type of unsupervised machine learning technique that uses backpropagation to adjust the target values to the inputs. Autoencoders have a habit of condensing the dimensions of our inputs into a more compact representation. If the first data is required, the condensed data will be used to recreate it. The purpose of an autoencoder is to train the model to ignore signal noise in order to discover a symbol for a set of knowledge, generally to reduce dimensions. They work by condensing the input into a latent-space description and then reconstructing the outcome from there. We'll visualize our findings and results as part of the analysis once both of these models have been implemented and trained, and we'll try and compare the trained models to see which one gives an exact result.

CONCLUSION

- AIM AND SCOPE
- ABSTRACT/PROBLEM STATEMENT
- OBJECTIVES (GAPS IDENTIFIED)
- SCHEDULE DIAGRAM OF THE SYSTEM
- BLOCK DIAGRAM OF THE SYSTEM/ARCHITECTURE OF THE SYSTEM
- SOLUTION FOR THE OBJECTIVES AND METRICS APPLIED
- RESULTS AND DISCUSSION WITH GRAPHS
- Implementation – [Demo] Video Recorded File
- GLOSSARY
- CONCLUSION

The one class classifiers we used in the project was used for both training and testing set with which it will segregate malicious and good traffic which comes through the network. To increase the efficiency of the one class classifiers we implemented a model using auto encoders which uses deep learning neural networks. By the use of both the algorithms we increased the efficiency of the project and we also attempted to overcome the problems that exists in the datasets, namely the class imbalance issue and the data being unrealistic, by avoiding the attacks data during training, the model was trained only using normal traffic, so it was not affected by the class imbalance of the dataset. Another strength of this approach is its simplicity, it consists of only a single hidden layer of 8 neurons making it very easy to train and especially suitable for online learning. During evaluation we avoided human manipulation of the threshold in order to achieve reproducible results without human interference

REFERENCES (MINIMUM 10 REFERENCES

- AIM AND SCOPE
- ABSTRACT/PROBLEM STATEMENT
- OBJECTIVES (GAPS IDENTIFIED)
- SCHEDULE DIAGRAM OF THE SYSTEM
- BLOCK DIAGRAM OF THE SYSTEM/ARCHITECTURE OF THE SYSTEM
- SOLUTION FOR THE OBJECTIVES AND METRICS APPLIED
- RESULTS AND DISCUSSION WITH GRAPHS
- Implementation – [Demo]-Video Recorded File
- GLOSSARY
- CONCLUSION
- REFERENCES (MINIMUM 10 REFERENCES

1. Intrusion detection using deep sparse auto-encoder and self-taught learning, Qureshi by A. S., Khan, A., Shamim, N., & Durad, M. H. (2019) Neural Computing and Applications (2019)
2. A Clustering-based Shrink AutoEncoder for Detecting Anomalies in Intrusion Detection Systems by Bui, T. C., Hoang, M., & Nguyen, Q. U. (2019, October) 2019 11th International Conference on Knowledge and Systems Engineering (KSE). IEEE, 2019.
3. A Modular Multiple Classifier System for the Detection of Intrusions in Computer Networks Giorgio Giacinto, Fabio Roli, Luca Didaci Department of Electrical and Electronic Engineering, University of Cagliari, Italy
4. A Clustering-based Shrink AutoEncoder for Detecting Anomalies in Intrusion Detection Systems Bui, T. C., Hoang, M., & Nguyen, Q. U. (2019, October) In 2019 11th International Conference on Knowledge and Systems Engineering (KSE) (pp. 1-5). IEEE.
5. A novel statistical analysis and autoencoder-driven intelligent intrusion detection approach Ieracitano, C., Adeel, A., Morabito, F. C., & Hussain, A. (2020). Neurocomputing, 387, 51-62.
6. J. K. Chahal, V. Gandhi, P. Kaushal, K. R. Ramkumar, A. Kaur and S. Mittal, "KAS-IDS: A Machine Learning based Intrusion Detection System," 2021 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021, pp. 90-95, doi: 10.1109/ISPCC53510.2021.9609402.
7. G. Yedukondalu, G. H. Bindu, J. Pavan, G. Venkatesh and A. SaiTeja, "Intrusion Detection System Framework Using Machine Learning," 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA), 2021, pp. 1224-1230, doi: 10.1109/ICIRCA51532.2021.9544717.
8. D. Xuan, H. Hu, B. Wang and B. Liu, "Intrusion Detection System Based on RF-SVM Model Optimized with Feature Selection," 2021 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), 2021, pp. 1-5, doi: 10.1109/CCCI52664.2021.9583206.
9. A. Aljohani and A. Bushnag, "An Intrusion Detection System Model in a Local Area Network using Different Machine Learning Classifiers," 2021 11th International Conference on Advanced Computer Information Technologies (ACIT), 2021, pp. 483-488, doi: 10.1109/ACIT52158.2021.9548421.
10. 0. H. Elbahadır and E. Erdem, "Modeling Intrusion Detection System Using Machine Learning Algorithms in Wireless Sensor Networks," 2021 6th International Conference on Computer Science and Engineering (UBMK), 2021, pp. 401-406, doi: 10.1109/UBMK52708.2021.9558928.

Paper IEEE Template

Title of the Paper
Authors Name(Students + Mentor Name)
Keywords
Introduction
LIterature survey
Methodology
Comparative study (if any)
Results and Discussion
Conclusion
References
Appendix (if any)
Biography (Authors)
No. of Pages (Min 10 to 20 pages)

Plagiaraism Report(<=12 %)- Any open source tool

Paper Communication Details
(ex: submitted/accepted/published)

https://drive.google.com/drive/folders/1QQ4b98J0qoIFA9gxD8PuaxD7Dhj0MHNI?usp=sharing


Thank
You