The Detection of a Ransomware attack on IoT devices deployed on Cloud Computing Environment Using Artificial Intelligence and Machine Learning

Temechu Girma Zewdie

University of the District of Columbia

Abstract

Detecting ransomware has become an important undertaking involving various sophisticated AI/ML solutions for improving security. To further enhance ransomware detection capabilities, this research paper will address the ransomware attack cybersecurity issues using a state-of-the-art solution approach and applying AI – Machine Learning techniques to design and develop a better AI machine learning (AI/ML) model using Random Forest that helps to classify and detect IoT-based ransomware attacks whether benign or ransomware, in a cloud computing environment, and enhance the existing solution and ensures the detection of a ransomware attack on IoT devices deployed on a cloud computing environment to secure data. Moreover, our research will present different statistical results generated from the security analysis, classification, and detection of IoT-based ransomware attacks on a cloud computing environment by describing how AI-ML Algorithms can be further implemented with existing multilayer security solutions to protect vital data from ransomware attacks. Finally, we will display and prove how our research approach closes the existing security gap and significantly mitigate the risk by showing a comparative analysis with other prior and current related research work.

Keywords: ***Cybersecurity, IoT, Ransomware Detection, Machine learning, Cloud Computing***

Objective of the research

1. To design a new AI machine learning model that helps to better classify and detect IoT-based ransomware attacks on a cloud computing environment.
2. To fill out a solution that ensures the detection of a ransomware attack on IoT devices deployed on a cloud computing environment to secure data
3. To undertake a security analysis, classification, and detection of IoT-based ransomware attacks on a cloud computing environment.

Methodologies

This research explores and profoundly analyzes the various AI/ML models to get maximum accuracy results

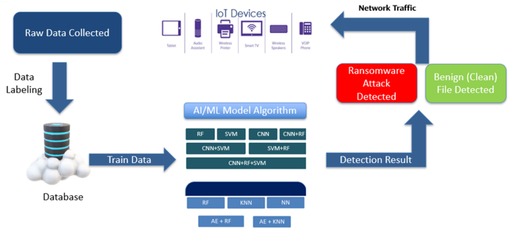
For the Preliminary assessment Phase:

- RF (Random Forest)
- SVM (Sector Vector Machine)
- CNN (Convolutional Neural Network)
- CNN + RF
- CNN + SVM
- RF + SVM
- RF + SVM + CNN

The Final Research Phase

- Random Forest (RF)
- K-nearest neighbors' algorithm (KNN)
- Neural Network(NN)
- Auto encoder (AE) +Random Forest(RF)
- Auto encoder (AE) + k-nearest neighbors (KNN)

High-Level ransomware Detection Architecture with AI/ML



Performance Evaluation Techniques

$$precision = \frac{TP}{TP+FP}$$

$$recall = \frac{TP}{TP+FN}$$

$$F1 = \frac{2 \times precision \times recall}{precision + recall}$$

$$accuracy = \frac{TP+TN}{TP+FN+TN+FP}$$

$$specificity = \frac{TN}{TN+FP}$$

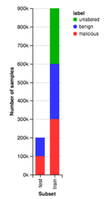
$$F1\ score = 2 * \frac{Precision * Recall}{Precision + Recall}$$

$$\text{Micro avg Precision} = \frac{TP1+TP2}{TP1+TP2+FP1+FP2}$$

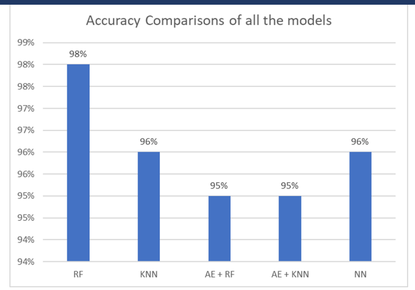
Where, TP, TN, FP, and FN indicate true positive, true negative, false positive, and false negative, respectively.

Research result

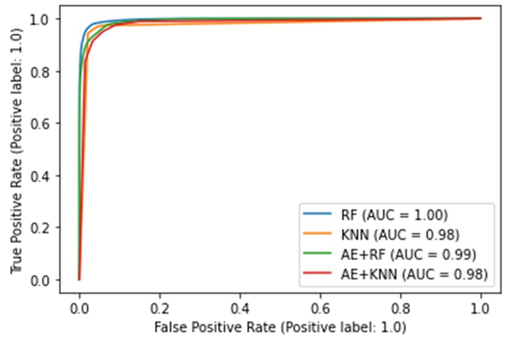
Distribution of Ransomware, benign, and unlabeled samples in the training and test set



Accuracy Comparison result of all the Models



ROC Curve (Area Under the Curve)



Conclusion and Future work

- Based on the comments received from the proposal defense and our research assessment result, we have narrowed down our approach (model) to get a maximum result.
- Besides, using more datasets, hyperparameters, and a grid search helped us to find the best parameters associated with the model.
- Based on the new AI/ML models we are better to better o classify and detect IoT-based ransomware attacks in a cloud computing environment.
- Moreover, we find out a solution that ensures the detection of a ransomware attack on IoT devices deployed on a cloud computing environment to secure data.
- Finally, in this research, we examined various models, and algorithms, security analyses to classify and detect IoT-based ransomware attacks on a cloud computing environment.

Future work

- In this research, we have used a static dataset. Thus, if the study expands to non-static data (real-time data), i.e., if the program is retrieved and analyzed in real time, we may get a different result.
- Our dataset is limited in the number of ransomware variants since we used the 2017/2018 collected dataset from Sophos' research lab. Therefore, if the updated version of the dataset included all ransomware variants, the result would be more lucrative.

Reference

[1] Y. Chen, "IoT, cloud, big data and AI in interdisciplinary domains," Simulation Modelling Practice and Theory, vol. 102, no. 102070, 2020.
[2] M. Patel, J. Shangkuan and C. Thomas, "McKinsey & Company," 13 01 2020. [Online]. Available: https://www.mckinsey.com/industries/semiconductors/our-insights/whats-new-with-the-internet-of-things. [Accessed 20 04 2021].
[3] K. L. Lueth, "IoT analytics," 08 08 2018. [Online]. Available: https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/. [Accessed 05 05 2021].
[4] NCTA, "Infographic: The Growth Of The Internet Of Things," 14 05 2014. [Online]. Available: https://www.ncta.com/whats-new/infographic-the-growth-of-the-internet-of-things. [Accessed 11 11 2020].
[5] E. P. Yadav, E. A. Mittal and H. Yadav, "IoT: Challenges and Issues in Indian Perspective," in 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU), Bhimtal, 2018.
[6] Z.-K. Zhang, M. C. Y. Cho, C.-W. Wang, C.-W. Hsu, C.-K. Chen and S. Shieh, "IoT Security: Ongoing Challenges and Research Opportunities," in 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications (SOCA), 2014.