Predicting Cyber Threats Using Data Mining and Machine Learning Techniques

- Research work done by Bhargava Teja Nuvvula # 10536703

> Data-mining and machine learning based techniques are important factors in detecting security threats

The main objective is to develop a solution that can perform the prediction on the Cybersecurity attacks on the IT environment so that we can take the required actions to safeguard the system even before the attack.

Research Questions

1. What would be the effective method to handle the attacks on the application by breaking the cybersecurity?
2. How we can anticipate the event of attacks on security with the help of analyzing the past incidents?
3. How the machine learning and data mining techniques can be used to solve the real-time problems by analyzing the existing data in the field of cybersecurity?

Methodology

We going to adopt KDD for our thesis which is otherwise known as Knowledge Discovery in Databases.

The process must follow the below stages:

- Selection
- Preprocessing
- Transformation
- Data Mining
- Interpretation/Evaluation

Dataset

The dataset was prepared by collecting the incident details from small and medium enterprises in South Korea and the classifier model will be trained with this dataset so that the model can perform the prediction on the cybersecurity incidents.

Implementation And Evaluation

Implementation - We did not have any specific technique that needs to be applied to perform intrusion detection. The possible algorithms would be decision tree, artificial neural networks, or even clustering techniques. On top of that, we have to develope a machine learning solution.

Evaluation- The classification model will be evaluated using the different evaluation metrics like the accuracy of the model, plotting a confusion matrix, calculating the precision score, and calculating the recall score value.

References

The survey of data mining applications and feature scope.,2012
Text clustering for digital forensics analysis., 2009
Naive Bayesian networks in intrusion detection systems., 2004

DBS
Dublin Business School
excellence through learning