Unsupervised Learning for Threat Detection

K. Yadav

National Insititute of technology, Kurukshetra

Using massive amounts of data to learn about different aspects of data and then using that knowledge to extract different types of information from unseen data has gained a lot of attraction in recent times. This methodology is known as Machine Learning. One of the massive successes of Machine Learning in recent times can be seen in network threat detection [1]. As different electronic devices are increasing, new and mutated threats are evolving rapidly, which are evading traditional blacklisting techniques of threat detection and prevention.

As these electronic devices are evolving rapidly, we are also seeing variation in their software and hardware level architecture [2]. These variations are due to the fact that the manufacturers of these electronic devices are distributed among a wide geographical region and there is no common worldwide standard regarding hardware and software requirements that must be embedded while manufacturing these devices. One such example is the Internet of Things (IoT). The OSI level architecture in IoT devices varies from three layers to five layers [2]. Figure 1 presents a variation in the OSI layer of four-layered and five-layered architecture along with the attacks present at different layers. When new layers and sensors evolve according to the consumer's requirement, it becomes very difficult to protect against vulnerabilities evolving from these new layers and sensor devices.

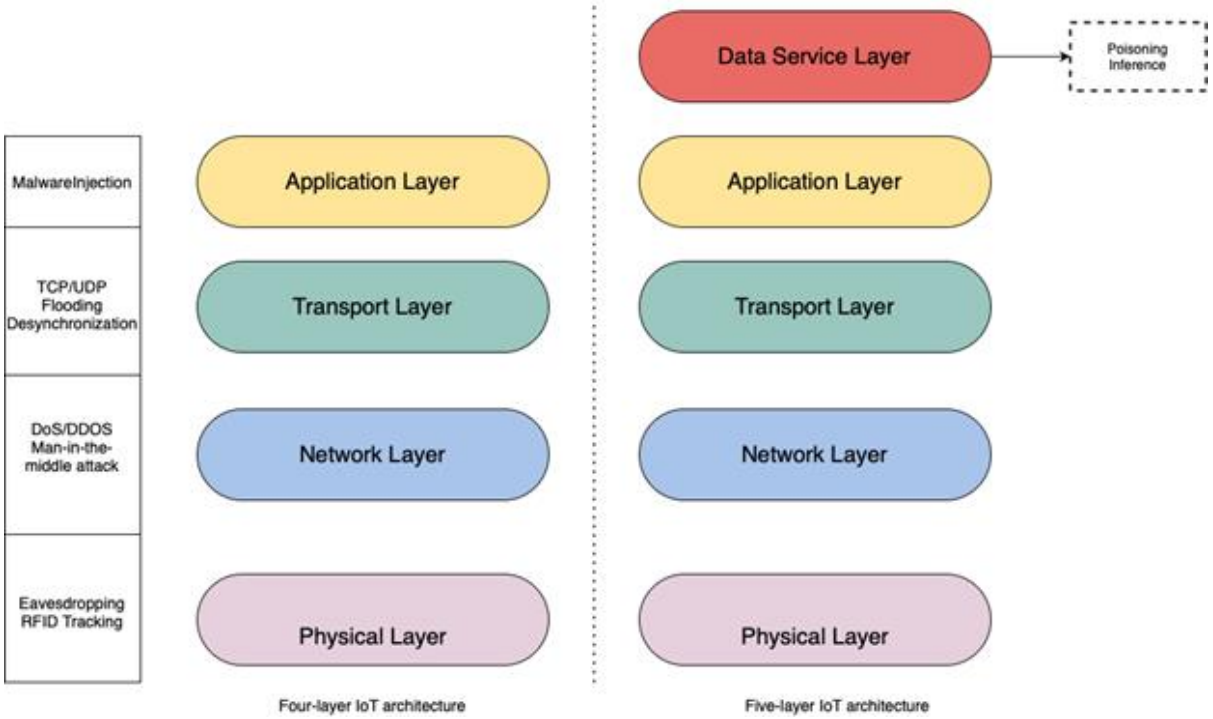

Fig 1: Variation in threats at different OSI Layer

Supervised machine learning needs labeled data to train a model. Whenever a supervised machine learning model built for the four-layer architecture is used to detect threats present in the five-layer architecture, it greatly fails, as the features present in the dataset of the five-layer architecture do not resemble the feature on which the machine learning model was trained. In Figure 1, models trained on four-layer architecture cannot detect

attacks like poisoning and inference on five-layer IoT architecture. To solve the problem, researchers have developed an automated approach called unsupervised machine learning. Unsupervised machine learning uses algorithms such as auto-encoders and the deep Boltzmann machine to train a machine learning model [3]. A great advantage of this approach over the supervised approach is that it does not need a labeled dataset. These algorithms can extract features from the dataset and convert raw data into a labeled dataset. The labeled dataset can then be used by any machine learning algorithm to detect threats. These algorithms can be useful for detecting threats to electronic devices irrespective of their architecture.

Open research problems:

- Unsupervised machine learning algorithms come with the risk of increased time complexity. As the raw dataset increases, the time to extract the features is also increases. [4].
- Extracting features by compressing the data from a higher dimension to a lower dimension may lead to a higher loss in data reconstruction. A wide range of research is being done to solve this issue [4].

References

1. Yuan, Fangfang, et al. “Insider threat detection with deep neural network.” *International Conference on Computational Science*. Springer, Cham, 2018.
2. Mrabet, Hichem, et al. “A survey of IoT security based on a layered architecture of sensing and data analysis.” *Sensors*20.13 (2020): 3625.
3. Wei, Yichen, Kam-Pui Chow, and Siu-Ming Yiu. “Insider threat detection using multi-autoencoder filtering and unsupervised learning.” *IFIP International Conference on Digital Forensics*. Springer, Cham, 2020.
4. Zhai, Junhai, et al. “Autoencoder and its various variants.” *2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*. IEEE, 2018.