Chapter 10

Future Research Directions

10.1 Future Research Directions

Future research into zero-day attack prediction may look at the method of improving the resilience of ML and DL models to adversarial attacks, such as robust training and robust optimization. Otherwise, the creation of algorithms that can easily dynamically modify the feature selection mechanisms to the evolving nature of networks, and research interests in the integration of multi-modal sources of data that generate more comprehensive threat intelligence. Future studies can be oriented to improving the interpretability of the predictive models based on explainable AI, addressing the issue of privacy based on privacy-preserving ML and DL, and the real-time response mechanism to prevent threats in advance. Moreover, by developing standard benchmark datasets and assessment processes, reproducibly and comparatively testing the results might be more readily available and this will accelerate the amount of research in the field. Under this kind of research, the various dimensions of effectiveness and reliability of the zero-day attack warning systems can be significantly enhanced in which the final output would be to enhance the robustness of the cyber security systems against the newly emerging threats.

Adversarial Attack Resilience: Research the techniques of making ML and DL models more resilient to adversarial attack when applied to zero-day attack prediction systems. This includes the investigation of the strong optimization schemes, the adversarial training schemes, and the model validation schemes in order to minimize the impact of the adversarial manipulations.

Dynamic Feature Adaptation: Discover how to come up with algorithms capable of dynamically changing feature selection mechanisms, as well as feature extraction mechanisms depending on the conditions of the network and the attacks. This involves incorporation of self adaptive learning mechanisms that constantly monitor and optimize feature relevancy, though real time feedback of the network.

Multi-Modal Data Fusion: Multi-modal data integration based on multi-modes, such as Network activity logs, Event logs, User activity logs, etc. to enhance the

completeness and power of zero-day attack prediction models. Research fusion technique, which may be adopted to effectively integrate data of different sources with a view of providing full threat data.

Explainable AI to Interpretability: The research of the ways of making ML and DL models more interpretable and explainable in terms of zero-day attacks prediction. Identify how to make model predictions easy to understand and interpret in a way that cybersecurity analysts can have a superior understanding of the decisions and be accountable to decisions made by an automated system.