ABSTRACT

The advent of the Internet of Things (IoT), with the consequent changes in network architectures and communication dynamics, has strongly conditioned the security market by radically shifting traditional perceptions of the current Internet toward an integrated vision of smart interconnected objects. However, due to their provided features and popularity, such devices have become one of the main targets for attackers who, exploiting several systems-related vulnerabilities and well-engineered applications, are able to conduct different hostile activities. For this reason, also thanks to the great success of Machine Learning (ML) and Deep Learning (DL) based techniques in the last decade, many innovative solutions have been proposed in order to counteract the exponential and yearly growth of malware applications. However, since the related detection models should provide an adequate generalization capability, their success strongly depends on the right choice of the employed features. To this purpose, new empowered strategies are needed to spot malware threats in several network security scenarios, with particular attention to those related to IoT and Federated environments, respectively.

Therefore, this thesis focuses on the enhancement of detection solutions that, due to the presence of many vulnerable and hardware-constrained devices, are characterized by several challenges regarding security and privacy. Under this vision, Chapter 1 presents a detailed overview of the state-of-the-art by highlighting the weaknesses of the existing approaches. Next, Chapters 2, 3, and 4 focus on the empowerment and effectiveness of such solutions by employing new dynamic and static-based feature representation techniques. Also, they highlight the capabilities of DL to offer sophisticated models capable of reducing Run-time damages and involving the computation capabilities of federated environments, respectively.

On the other hand, due to the recent explosion of IoT-related malware applications and the necessity of protecting privacy, the thesis extends its focus to malware detection activities in Federated organizations. Therefore, Chapter 5 proposes a new Markov Chains-based detector capable of improving the most famous Federated Learning (FL) based solutions. To this purpose, a dedicated privacy-preserving architecture is employed, in which the involved clients build the related detection model by indirectly sharing the analyzed applications. Finally, Chapter 6 presents the Conclusions about the reported contributions by highlighting possible and relevant future research directions.