Abstract

The rapid proliferation of Internet of Things (IoT) devices has significantly transformed various sectors by enabling enhanced connectivity and automation. However, this expansion has concurrently introduced substantial cybersecurity challenges, as the increasing number of interconnected devices broadens the potential attack surface. To safeguard these complex and distributed IoT-edge environments, there is an urgent need for robust and efficient Intrusion Detection Systems (IDSs) specifically tailored to address the unique constraints and requirements of IoT deployments. One critical aspect in developing effective IDSs for IoT-edge environments is the availability of short yet representative datasets. These datasets are essential for training lightweight IDS models directly on resource-constrained IoT-edge devices, thereby minimizing energy consumption during on-board training processes. Traditional IDS models often require extensive computational resources and large datasets, which are impractical for deployment on microcontroller units (MCUs) commonly used in IoT devices. Therefore, leveraging reduced and highly relevant datasets, coupled with optimized network architectures, is imperative to achieve efficient and scalable intrusion detection. In response to these challenges, this paper presents a comprehensive performance assessment of an Intrusion Detection System based on a Siamese Neural Network (SNN) deployed on a compact Microcontroller Unit (MCU). The SNN architecture is chosen for its ability to learn similarity metrics, which are crucial for identifying anomalous traffic patterns indicative of IoT-specific attacks. The study begins with the creation of a realistic IoT dataset, meticulously gathered from actual IoT devices and encompassing a wide range of benign and malicious traffic scenarios. This dataset is then benchmarked against existing state-of-the-art datasets to ensure its robustness and representativeness. The primary objective of this research is to evaluate the efficacy of the SNN-based IDS in detecting intrusions while operating within the stringent computational and power limitations of MCU platforms. To achieve this, several key performance metrics are analyzed, including detection accuracy and processing latency. The dataset facilitates the training and testing of the SNN, allowing for a detailed examination of its ability to discern subtle anomalies in network traffic that may signify potential security breaches. Experimental results demonstrate that the SNN-based IDS achieves a high detection rate, effectively identifying a wide array of IoT-specific attacks with minimal false positives. Moreover, the system operates efficiently within the computational constraints of the MCU, maintaining low processing latency and minimal energy consumption. These findings underscore the practical applicability of the proposed IDS in real-world IoT-edge environments, where resource efficiency and rapid threat detection are paramount. Additionally, the implementation of the SNN on an MCU highlights the feasibility of deploying advanced neural network models on low-power devices without compromising performance. This advancement paves the way for more sophisticated and intelligent security solutions in IoT ecosystems, enhancing their

resilience against emerging cyber threats. In conclusion, this study not only validates the effectiveness of the SNN-based IDS in securing IoT-edge environments but also contributes a valuable, realistic dataset to the research community. The integration of efficient neural network models with optimized datasets offers a promising pathway towards robust and scalable cybersecurity measures for the ever-expanding landscape of IoT devices. Future work will explore further optimizations and extensions of this approach, aiming to enhance detection capabilities and extend applicability to a broader range of IoT scenarios.