International Journal of Computer Science and Engineering(IJCSE)
ISSN (P): 2278–9960; ISSN (E): 2278–9979
Vol. 13, Issue 1, Jan–Jun 2024; 265–278

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

ADAPTIVE DEEP LEARNING-DRIVEN INTRUSION DETECTION AND PREVENTION FRAMEWORK FOR SECURING IOT NETWORKS AGAINST EVOLVING CYBER THREATS

Kuppili Shubham[1] & Rakesh Verma[2]

[1]Ph.D. Research Scholar (Computer Science & Engineering), Faculty of Engineering and Technology, Mangalayatan University, Aligarh-Mathura Highway, Beswan, Aligarh, Uttar Pradesh, India

[2]Assistant Professor, Faculty of Engineering and Technology, Mangalayatan University, Aligarh-Mathura Highway, Beswan, Aligarh, Uttar Pradesh, India

ABSTRACT

The rapid expansion of Internet of Things (IoT) networks has transformed conventional computing and communication environments by connecting a diverse range of sensors, embedded devices, smart appliances, industrial controllers, healthcare systems, and intelligent infrastructure. However, the continuous exchange of data among resource-constrained devices creates an extensive attack surface that can be exploited through denial-of-service attacks, distributed denial-of-service attacks, botnet activities, probing, credential-based attacks, malware propagation, spoofing, and other emerging cyber threats. Conventional intrusion detection and prevention mechanisms often experience difficulties in identifying sophisticated and previously unseen attack patterns because they depend heavily on predefined signatures, manually selected features, or static detection rules. This research proposes an adaptive deep learning-driven intrusion detection and prevention framework designed to strengthen the security and resilience of IoT networks against evolving cyber threats. The proposed approach employs deep learning models to learn complex relationships within network traffic and device communication behaviour, enabling automated extraction of discriminative characteristics from large-scale and heterogeneous IoT traffic. The framework incorporates data preprocessing, feature transformation, traffic classification, abnormal behaviour identification, and automated prevention mechanisms within an integrated security architecture. Normal and malicious network activities are analysed continuously, while the adaptive learning component enables the detection model to respond to changes in traffic characteristics and emerging attack behaviour. To improve practical applicability, the framework considers the computational and communication limitations of IoT environments and supports security decisions that can be implemented at appropriate network or edge locations. The effectiveness of the proposed framework can be assessed using established IoT cybersecurity datasets and representative attack scenarios through metrics such as accuracy, precision, recall, F1-score, false-positive rate, detection latency, and prevention response time. Particular attention is given to maintaining a balance between detection capability and computational overhead, since excessive processing requirements can adversely affect resource-constrained IoT devices. The proposed framework is expected to provide more reliable identification of both known and evolving attacks while reducing unnecessary security alerts and enabling faster preventive responses. By combining adaptive deep learning with intrusion detection and prevention, the study contributes toward the development of intelligent, scalable, and resilient security mechanisms capable of protecting heterogeneous IoT networks in increasingly dynamic cyber threat environments.

KEYWORDS: *Internet of Things (IoT); Deep Learning; Intrusion Detection; Intrusion Prevention; Cybersecurity*

Article History

Received: *10 Mar 2024* | ***Revised:*** *13 Mar 2024* | ***Accepted:*** *27 Mar 2024*