Notification Number: 584/2025

Date: 18/08/2025

Name of the Scholar: Syed Ali Mehdi

Name of the Supervisor: Prof. Syed Zeeshan Hussain

Name of the Department: Department of Computer Science

Name of the Faculty: Faculty of Sciences, JMI, New Delhi

Topic of the Research: An Intelligent Intrusion Detection System for IoT Based Environment

Findings

The research successfully developed a hierarchical, AIS-IDS model for securing the IoT environments. The AIS-IDS model uses the concept of the artificial immune system (AIS) with unsupervised learning techniques like DBSCAN clustering to efficiently detect cyber threats. The model achieved an accuracy of 82.81%, overcoming the accuracy of the traditional classifiers such as SVM (71.69%) and Naïve Bayes (77.31%), indicating its capability to detect diverse IoT-based attacks with greater precision.

The findings revealed that the AIS-IDS model makes use of LPUs for edge-based detection and its CPU for centralized intelligence processing enhances the detection speed and accuracy while reducing the communication overhead typically noticed with centralized IDS models. The Security by Design approach, by Industrie 4.0, was achieved by embedding IDS mechanisms at multiple layers of the IoT infrastructure.

The AIS-IDS model is able to strongly classify benign traffic, C&C, C&C-FileDownload, C&C-HeartBeat, and Okiru attacks with perfect precision and recall. But when it comes to the DDoS attacks, it has a 48% recall, which means that more than half of the actual DDoS attacks were misclassified by the AIS-IDS. For zero-day attacks, the AIS-IDS model gives 56% precision and 53% recall, which means that nearly half of the detected zero-day attacks might be false positives, while also missing a significant number of actual zero-day threats. But when the confusion matrix is noticed it reveals that most of the portion of zero-day attacks were misclassified as general "Attack" traffic. Thus, it is able to mark zero-day attacks as an attack pattern and not a Benign pattern, which is beneficial for the end user. It did not mark the Zero-day attacks as a normal pattern but put them under the class of Attack. This is a positive finding suggesting that it does not consider the abnormal Zero-day attack as normal traffic and allows them to pass to the system. But still, the label outcome is wrong. This highlights the need for further optimization of feature selection and training techniques. But the proposed AIS-IDS approach demonstrated promising potential for real-world IoT security applications, offering a scalable, adaptive, and intelligent intrusion detection solution.