**PROPOSED SYSTEM**

The proposed system aims to overcome the limitations of the existing approach by introducing several enhancements to strengthen IoT network attack detection using artificial intelligence. Firstly, the system proposes the incorporation of a more diverse set of labeled datasets, beyond the Aposemat IoT-23 dataset, to ensure a comprehensive understanding of evolving attack patterns. This expansion enables the system to generalize better and recognize novel threats that may not be covered by a single dataset.

Secondly, the proposed system advocates for the integration of dynamic and adaptive machine learning models that can evolve with the changing nature of IoT attacks. This may involve exploring deep learning techniques or other advanced algorithms capable of capturing intricate patterns and adapting to emerging threats in real-time.

Thirdly, the proposed system emphasizes the development of a more scalable architecture, considering the increasing scale and complexity of IoT networks. This could involve the implementation of distributed computing techniques or lightweight algorithms suitable for resource-constrained IoT devices, ensuring efficient and effective network attack detection at scale.

Additionally, the proposed system suggests leveraging anomaly detection methods alongside traditional classification approaches to enhance the detection of previously unseen attacks. Anomaly detection can identify deviations from normal network behavior, providing a proactive defense against emerging threats not explicitly defined in the training dataset.

Lastly, the proposed system aims to optimize feature engineering processes to minimize computational overhead. This involves refining preprocessing techniques to strike a balance between improving detection accuracy and ensuring efficient resource utilization, particularly in the context of IoT devices with limited computational capabilities. Overall, the proposed system seeks to advance the state-of-the-art in IoT network attack detection by addressing existing limitations and embracing more dynamic, scalable, and adaptable approaches.

**ADVANTAGES**

**Improved Detection Accuracy:** The proposed system leverages a more diverse set of labeled datasets and advanced machine learning models, contributing to enhanced detection accuracy. This ensures a comprehensive understanding of various IoT attack patterns and improves the system's ability to recognize and classify both known and emerging threats.

**Adaptability to Dynamic Threats:** By incorporating dynamic and adaptive machine learning models, the proposed system can better adapt to the evolving nature of IoT attacks. This adaptability allows the system to recognize and respond to new and previously unseen threats in real-time, providing a more proactive defense mechanism.

**Scalability for Large IoT Networks:** The proposed system addresses scalability challenges by introducing a more scalable architecture. This ensures efficient performance in large-scale IoT networks, accommodating the increasing number of devices and complexities in network structures without compromising the system's ability to detect and respond to security threats.

**Comprehensive Defense with Anomaly Detection:** The integration of anomaly detection methods alongside traditional classification approaches adds a layer of comprehensive defense. Anomaly detection enables the system to identify deviations from normal network behavior, offering a proactive defense against novel and unexpected attacks that may not be explicitly defined in the training dataset.

**Optimized Resource Utilization:** The proposed system optimizes feature engineering processes to minimize computational overhead. This optimization ensures efficient resource utilization, making the system more suitable for deployment in resource-constrained IoT devices. By balancing detection accuracy and computational efficiency, the proposed system maximizes its effectiveness without putting undue strain on device resources.