

## **Communications in Computer and Information Science**

### **IoT smart home security: Improving cyberattacks detection with stacked ensemble methods**

Abu-Mahfouz, Adnan MI

Council for Scientific and Industrial Research (CSIR)

Meiring Naude Drive, Pretoria, 0184

Email: AAbuMahfouz@csir.co.za

The Internet of Things (IoT) has created some remarkable changes, especially in smart homes. However, this increased connectivity has also heightened the exposure of IoT devices to cyber threats. Machine learning methods often struggle with a lack of robust datasets and employ single models to detect various attacks. This limitation significantly reduces the models' detection accuracy, increases false positive rates, and impedes robustness against evolving threats, adaptation to changes, and efficient handling of different devices. Therefore, this paper proposes a robust stacked ensemble model designed to effectively detect and classify cyberattacks in IoT-based smart homes. Utilizing a novel real-world dataset, we trained and evaluated four ensemble algorithms: Random Forest (RF), Extreme Gradient Boost (XGBoost), Extra Trees (ET), and Adaptive Boosting (AdaBoost) using various performance metrics. The results reveal that XGBoost and RF outperformed the others and were selected as base estimators for the stacked ensemble model. Our model achieved an impressive 99% accuracy in detecting various cyberattacks, such as Distributed Denial of Service (DDoS), Denial of Service (DoS), and Mirai. It also demonstrated excellent performance in identifying DDoS and DoS attacks, with F1 scores exceeding 99%. Despite challenges with detecting Brute Force and Web-based attacks, likely due to data imbalance, the overall results demonstrate the effectiveness of the proposed approach. By utilizing the strengths of multiple models, the stack ensemble method significantly improved detection accuracy and efficiency in IoT ecosystems.