**Detecting Botnet Attacks in IoT Environments: An Optimized Machine Learning Approach**

**Project Introduction**

IoT (internet of things) network consist of self-organizing tiny devices which will sense data from its environment and then send to centralized server for monitoring some examples of IOT devices are Patient Health Monitoring IOT which will sense patient pulse and temperature and then report to hospital, Road side traffic monitoring, agriculture field temperature monitoring, smart home monitoring and many more.

The advantages of IOT will get affected when its network get hacked where malicious programmers can inject fake IOT devices in a network where this fake IOT will gather data from legitimate IOT and report to hacker or it may receive and send false data to centralized server whose monitoring decision will get wrong. In presents situation number of IoT attacks increased by 32% compare to year 2018. Hence, there is an immediate requirement for appropriate effective and efficient attack detection and mitigation techniques in such situations. Machine learning (ML) has arose as one possible solution due to the plenty of availability of IoT generated data which can be used to train ML models and this model can be used to detect attack from future IOT network data. Therefore, ML can be adopted for intrusion detection for IoT environments.

In propose work we are employing an optimized ML-based technique which is a combination of Bayesian optimization Gaussian Process (BO-GP) algorithm and decision tree (DT) classification model for accurately detection of attacks on IOT network. Propose algorithm performance is measure on Bot-IoT-2018 dataset and this algorithm witness high accuracy compare to those algorithms implemented in the past.

**Literature Review**

In the past many algorithms was introduced to tackle attacks on IOT environment but all this techniques has some advantages and dis-advantages over one and other. Li et al. proposes [1] a tree based classification model to detect attacks on intelligent transportation IoT environment. This work utilizes averaging feature selection technique using tree structure Machine Learning models to enhance the efﬁciency of the IDS detection. Mohammad Noor Injadat proposes [2] a multi stages based optimized Machine Learning based IDS system that maximize the prediction accuracy and minimize the computational complexity but this work lack of features optimization algorithms so it cannot be deployed on any real time environment. Srisivasubbramanyan BS [3] proposes a Schnorr signature based IOT attack detection where all legitimate IoT will interact with each other using Schnorr signatures and if any destination IoT received incorrect packet then it will result into incorrect signature and attack will be detected. Schnorr based signature detections are easy to implement but if attacker understand signature then he can alter signature itself as per tamper packet. Khalid Alissa proposes [4] IOT bot attack detection model based on SMOTE over-sampling and under-sampling and then evaluate performance using many machine learning algorithms. ML algorithms fully dependent on dataset and if dataset is accurate then it’s performance can be high, if data is inaccurate then ML will face issues of data Imbalance, over and under fitting and in such scenarios SMOTE can be useful in avoiding degradation of ML performance. In this work author has not provided any optimizations techniques so it cannot be deploy in real environment. Chaw Su Htwe proposes [5] CART based algorithm to mitigate IOT attack and this CART algorithm was trained on N-BaIoT IDS dataset and manages to get an accuracy of 99% compare to its counter algorithms like Naïve Bayes. Tarek Gaber proposes [6] a injection attack detection model which is utilizing two different features selection algorithms like Constant Removal and Recursive Features Elimination and then selected features were trained on different ML algorithms like SVM and decision tree and then author manages to get an accuracy of 99% on 8 selected best features. Yakub Kayode Saheed [7] has utilized modern-day UNSWNB-15 dataset to train ML algorithms like XGBOOST, SVM and manages to get an accuracy of 99.95 and 99.97%.

**Method / Proposed Approach**

In propose work we are employing an optimized ML-based technique which is a combination of Bayesian optimization Gaussian Process (BO-GP) algorithm and decision tree (DT) classification model for accurately detection of attacks on IOT network. Propose algorithm performance is measure on Bot-IoT-2018 dataset and this algorithm witness high accuracy compare to those algorithms implemented in the past.

We are utilizing techniques like MIN-MAX scaling for features normalization and then employing SMOTE technique to overcome under or over sampling issues. Normalized features further optimized by utilizing technique called “Bayesian Optimization Gaussian Process”. Optimized features will get trained with decision tree machine learning algorithm to predict IOT data as normal or attack.

**Potential Ethical or Legal Issues**

Here we have trained model with optimized Bayesian techniques and this techniques must kept secret from other clients as if attackers knows of this concept then they can attack trained model to report false prediction which can result into complete failure of the model.

**References**

1. Tree-based Intelligent Intrusion Detection System in Internet of Vehicles

2. Bayesian Optimization with Machine Learning Algorithms Towards Anomaly Detection

3. ESWSIoT: Enhanced Secure Communication by Detecting and Removing Wormhole Attack using Schnorr Digital Signature in IoT Networks. P. Deepavathi, Srisivasubbramanyan BS, C. Mala

4. Botnet Attack Detection in IoT Using Machine Learning. Khalid Alissa, Tahir Alyas, Kashif Zafar

5. Botnets Attack Detection Using Machine Learning Approach for IoT Environment. Chaw Su Htwe, Yee Mon Thant and Mie Mie Su Thwin

6. Injection attack detection using machine learning for smart IoT applications. Tarek Gaber, Amir El-Ghamry, Aboul Ella Hassanien

7. A machine learning-based intrusion detection for detecting internet of things network attacks. Yakub Kayode Saheed, Aremu Idris Abiodun, Sanjay Misra, Monica Kristiansen Holone, Ricardo Colomo-Palacio