Intelligent IoT Security using Fuzzy Optimum path forest classifier

Vignesh Raam S R

January 2023

Far Flew IoT

In the Current world Scenario, each and everything we are looking for in one way or another has used up the IoT technology in it. From Fitness Bands to even auto-pilot Cars.

Need For Security

Now Think what if some stranger comes to get his hands over your Tesla's run time Data and manipulates those values and feeds it back!! Well, then you wouldn't even be alive. IoT Security is a must not just here but in many other cases like critical IoT tasks in the Military and Industry.

How To detect Intrusions ??

In the last decades, machine learning (ML) techniques have been applied for Cyber-attack detection in IoT environments. The objective of these works is to find solutions that can prevent, detect, or mitigate attacks on this type of network. There are several works have been done using machine learning algorithms to build Intrusion Detection Systems (IDS)

1. intrusion detection system based on distributed machine learning using Blockchain technology.
2. The classification technique - support vector machine (SVM) was trained using the datasets obtained from each of the nodes of the IoT network.
3. IDS model based on DL and ML to overcome security attacks in IoT networks, using K-Nearest Neighbor (KNN), and Long Short-Term Memory (LSTM)
4. Random Forest to select important dataset features and Classification and Regression Trees (CART) to classify different attack classes

5. a model called Fuzzy Intrusion Detection System for IoT Networks (FROST). FROST uses the basis of fuzzy theory to make learning models more flexible, seeking to improve performance in the classification of imprecise data.

6. Fuzzy Optimum-Path Forest (Fuzzy OPF) is a variant of the OPF classifier designed as a pattern recognition technique

Fuzzy Optimum-path Forest Approach

Firstly Fuzzy logic is where we have classified classes based Degree of Truth We try to apply that logic for all Required points. Each sample will have a value that will be calculated with the help of a function whose one Parameter is the density of the sample. The Forest is nothing but a Graph G(N, A).

where, N is a grouping of Training class nodes and A is a set of edges connecting the Nodes in N

The Grouping of the Training data into samples whose density is calculated using the below function

$$\text{p(s)} = \Sigma((\sqrt{1/2\Pi\psi^2k}) * exp - d^2(q,u)/2\psi^2)$$

for all u ϵ A(q)

where A(q) is KNN of a sample q

ψ = **df/3 where df is the highest**

value between the edge of the graph

For scaling the input values the algorithm uses of Fuzzy Membership whose function is given Below:

$$F(q) = (1-\sigma) * (P(q) - Pmin)/(Pmax - Pmin) + \sigma$$

Now We also need a Path Cost function which is gonna say whether a path is present in the prototype data The function for that is Below:

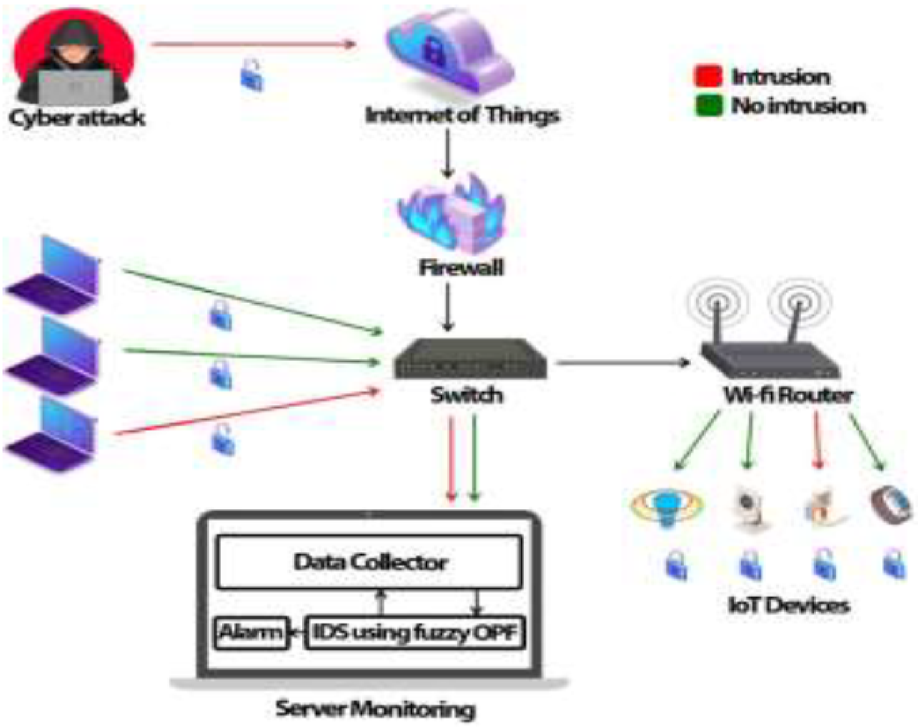
F max(u) =

$$\begin{cases} 0 & if x \epsilon T \\ +\infty & Otherwise \end{cases}$$

Fmax(ϕ * $< q, u >$) = min(F(u) * max(p(q),d(q,u))) For all qϵ N

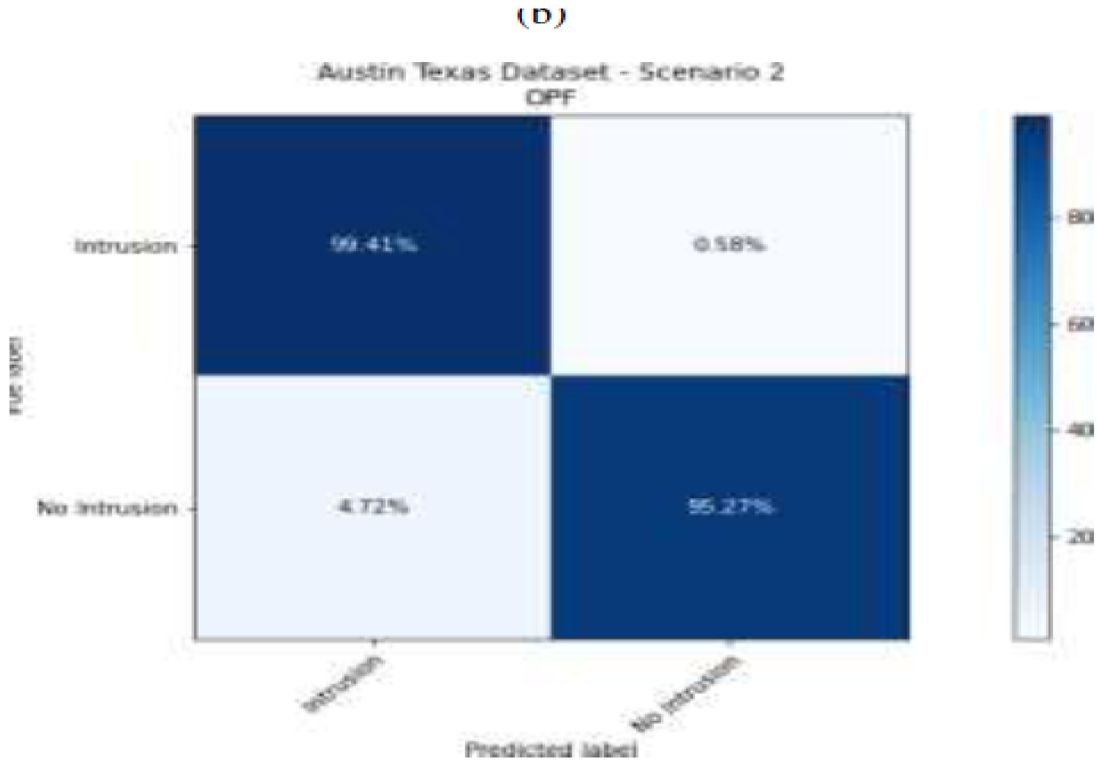
Proposed approach

The Switch is the only way through which all the devices are connected Using that switch we can get the network traffic and give it to the intrusion monitor (Fuzzy OPF) . It detects the intrusion and alerts the user



Conclusion

There using Fuzzy OPF we can find whether there is some sort of intrusion from the outside world and we lead a more secure privacy Also, the if we see the Confusion Matrix of Fuzzy OPF we can see that it is Highly Accurate. Also If we want to we can do Hyper Parameter Tuning to further increase the result. But of course more accurate the Training data The Better Detection!!!


(b)
Austin Texas Dataset - Scenario 2
OPF
Intrusion
No Intrusion
True label
Intrusion
No Intrusion
Predicted label