ISSN 2278-3091
Volume 12, No.6, November - December 2023
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse031262023.pdf
https://doi.org/10.30534/ijatcse/2023/031262023

A Hybrid Intrusion Detection Model to Alleviate Denial of Service and Distributed Denial of Service Attacks in Internet of Things

Samera Uga Otor[1], Beatrice Obianiberi Akumba[2], Adekunle Adedotun Adeyelu [3], Isaac Terngu Adom[4], Caleb Dese Iornongo[5] and Joseph Sunday Idikwu[6]
[1]Department of Mathematics/ Computer Science Benue State University Makurdi, Nigeria, sotor@bsum.edu.ng
[2]Department of Mathematics/ Computer Science Benue State University Makurdi, Nigeria, beatriceakumba@gmail.com
[3]Department of Mathematics/ Computer Science Benue State University Makurdi, Nigeria, adeyeluadekunle@yahoo.com
[4]Department of Mathematics/ Computer Science Benue State University Makurdi, Nigeria, iadom@bsum.edu.ng
[5]Department of Mathematics/ Computer Science Benue State University Makurdi, Nigeria, calebde@gmail.com
[6]Department of Mathematics/ Computer Science Benue State University Makurdi, Nigeria, josephinnocent99@gmail.com

Received Date : October 17, 2023 Accepted Date: November 26, 2023 Published Date: December 06, 2023

ABSTRACT

The Internet of Things (IoT) refers to a network of interconnected smart devices. The growth of IoT devices has increased the vulnerability of the network to attacks, such as Denial of Service (DoS) and Distributed Denial of Service (DDoS). Denial-of-Service (DoS) attacks are malicious activities aimed at rendering a computer network, system, or online service unavailable to legitimate users. This research addresses the growing vulnerability of IoT networks to DoS/DDoS attacks by developing a hybrid intrusion detection model to detect these attacks. The model integrates Kalman Filter (KF) with Artificial Neural Network (KF-ANN), Random Forest (KF-RF), Support Vector Machine (KF-SVM) and K-Nearest Neighbor (KF-KNN) machine learning models. The Kalman filter is an efficient tool for estimating the state of a system especially in the midst of uncertainty. Kalman filter was used to estimate the state of the system while the machine learning models were used to make predictions based on the estimated state to detect attacks in IoT. The model was tested using the DoS/DDoS Message Queueing Telemetry Protocol (MQTT) IoT dataset. Results shows Receiver Operative Curve Area Under the Curve (ROC-AUC) of 0.99% for KF-ANN and KF-RF, 0.98% and 0.97% for KF-KNN and KF-SVM. Detection accuracy of approximately 0.96%, 0.94% and 93% for KF-RF and KF-ANN, KF-KNN and KF-SVM respectively

Key words: ANN, Attacks, DoS/DDoS, Internet of Things, Kalman filter, Vulnerability.

1. INTRODUCTION

The Internet of Things (IoT) is a network of intelligent computing devices that connects and communicates wirelessly. IoT devices ranges from simple sensors that monitor environmental changes in temperature, pressure and humidity among others to mission critical devices. The Internet of Things (IoT) has advanced from its adoption in traditional sensing to crucial and essential applications. it is now recognized as the inspiration underlying today's technological shift and provides a means to capture data in real time [1]. Therefore, the number of IoT devices have shown continuous growth over the years. As at 2019, there were 7.4 million machines to machine (M2M) connected IoT devices which was further predicted to reach 29.3 billion by 2023 [2]. The rapid growth and proliferation of IoT devices has led to the increase in the number of potential entry points for attackers making these networks more prone to various types of attacks such as Denial of service and Distributed Denial of service (DoS and DDoS). Therefore, a lot still needs to be done to lighten the security vulnerabilities found in IoT devices

Denial-of-Service (DoS) attacks are malicious activities aimed at rendering a computer network, system, or online service unavailable to legitimate users. While, DDoS is an advance DoS attack in which several devices recruited to perform DoS attack (botnet) launch a DoS attack on the same target in other to interrupt or stop a legitimate service [3]. Though several DoS/DDoS detection mechanisms exist, there is still room for improvement as attackers keep devising new means of breaching existing solutions using new attack patterns.

The Kalman Filter has been used in computing for robotics [4], signal processing, tracking, among others. It is especially effective in cases where the state of a system must be approximated in the presence of anomalous behavior and ambiguity in the system. By integrating observations and predictions, the Kalman Filter can determine the condition of a system. While the Kalman filter is widely used for state estimation and tracking in various applications, it is not specifically designed for intrusion detection. However, the Kalman filter can be a part of a broader intrusion detection system, particularly when used in combination with other algorithms and methodologies. For example, the Kalman filter may be utilized for tracking the state of a system, and the estimated state variables can be fed into an intrusion detection algorithm that analyzes the system's behavior and identifies potential intrusions based on predefined rules or machine

learning models such as ANN, RF, KNN, among others. In the context of IoT networks, the Kalman filter can be used to estimate the behavior of network traffic and detect anomalies that may be indicative of DoS and DDoS attacks [5]. Therefore, integrating KF into other machine learning models can improve the accuracy and efficiency of the predictive model.

The remaining sections of the paper are; section two which reviews related literatures regarding this research, section three describes the methodology employed to develop the hybrid model, section four presents the results obtained and in section five the summary of the entire work and suggested future work is presented.

2. LITERATURE REVIEW

The integration of Kalman Filter and ANN have been proposed in various fields, including navigation systems and robotics. Recent research has shown that the integration of Kalman Filter and ANN can improve the performance of prediction models in various domains, including health care, finance, and transportation. According to [6], hybridizing the two models outperforms using the Kalman filter or neural network as standalone solutions in accuracy efficiency and simplification. Moreso, neural networks may establish the effectiveness of Kalman filter state-space equations in nonlinear systems.

The accuracy of object localization was determined to be higher using the ANN technique than with the KNN technique in [5]. As a result, the ANN-determined object coordinates were subjected to Kalman filtering. The results revealed that using ANN and Kalman Filtering enhanced localization accuracies and reduced localization error distances by 46%.

For efficient data cleaning and feature selection, [7] used Kalman filter to handle missing values and outliers. The filtered data was further subjected to a feature selection process using an evolutionary method called the “improved inertia weight-based dragonfly optimizer” to enhance the dataset. The selected features were then trained and classified using a deep learning algorithm known as “deep bagging based convolutional neural network DBCNN”. The NSL KDD dataset was used for this system, and comparative analysis with modern algorithms showed superior accuracy of 99.11% and low false positive rate of 0.8%.

Using system identification, [8] described two detection techniques for detecting optical fiber incursions under windy situations. The first approach, termed "state parameter comparison," involves generating the noise covariance matrix at each point using system identification and then comparing the normalized Frobenius norm of the noise covariance differences. The "cross reconstruction algorithm," the second algorithm, used non-intrusion point data to get system parameters via system identification. Kalman filter was then used to rebuild the signal, and the mean square error between the actual data and the rebuilt signal was compared. Simulation results indicated that both algorithms effectively detected intrusion points. However, there were trade-offs. The "state parameter comparison" algorithm required more time for calculations but exhibited better resistance to environmental interference. On the other hand, the "cross reconstruction algorithm" was faster but somewhat less robust.

Reference [9] introduced an intelligent DDoS intrusion detection model that combined a Kalman backpropagation neural network with the benefits of both error backpropagation and Kalman filtering. During the forward propagation of the neural network the Kalman filter was used to calculate and update the weight gain for each layer in response to the input data. The proposed DDoS intrusion detection model achieved an average detection accuracy of 94% with a low false alarm rate of 0.0952. The detection rate and precision for DDoS attacks were reported at 97.49% and 91.22%, respectively. However, it's worth noting that the Kalman filter was used to update the weight and the evaluation was based on a single dataset. Therefore, future work aims to enhance the model's security against DDoS attacks using different datasets and extend its capabilities to detect other types of IoT intrusions, such as Botnet attacks.

To ensure the security of Industrial Cyber-physical Systems (ICPSs) in Industry 4.0., [10] presented a hierarchically distributed intrusion detection scheme designed to provide comprehensive protection for ICPSs, considering three layered structure and various types of attacks. The layers are the physical system layer, the cyberspace layer and application control layer. At the physical layer, prospective and hidden attacks on the physical system were detected using a collection of sensory system with conditioned lingering anomaly monitoring. This monitoring was based on a process noise and measurement noise-adaptive Kalman filter (PNMN-AKF), which aided a joint systematic approximation of system states and noise covariance matrices. At the Cyberspace Layer, potential cyber-attacks were identified by monitoring the numerical dispersal of network transmission characteristics in the data transmission layer. This was achieved through a recursive Gaussian mixture model with a forgetting factor (FF-RGMM). While at the Application Control Layer, a “regularized sparse deep belief network model” was introduced to detect prospective attacks by describing misuse behavior. The proposed intrusion detection method was validated through extensive experiments on mathematical simulation systems and a comprehensive ICPS simulation platform. The results showed that the hierarchically distributed approach effectively recognizes prospective and hidden cyber-attacks in ICPSs while maintaining low false alarm rates and missing detection rates.

Reference [11] addressed the security concerns of the Internet of Things (IoT), with a particular focus on the Internet of Mobile Things (IoMT). The study introduced a novel approach to combine anomaly detection and intrusion detection in Internet of Mobile Things (IoMT) by developing a “Kalman filter and Cauchy clustering algorithm”. These were used for authenticating nodes in IoMT, by employing the Extreme Learning Machine classifier. The Kalman Filter was used to estimate pedestrian trajectories in an indoor environment by combining data obtained from a WiFi and Inertial Measurement Unit (IMU) to detect anomaly behavior in IoMT based on the estimated trajectories. The algorithm's performance was evaluated using the TamperU dataset for WiFi fingerprinting and the KDD99 dataset for intrusion detection. The results were compared with benchmark algorithms, and they demonstrated superior performance in terms of classification metrics.

Reference [12] proposed "an ensemble model based on weighted voting mechanism for intrusion detection". It combined a learning mechanism based on automated machine learning obtained by optimizing a deep neural network using a Bayesian Optimization with a prediction model built on the Kalman filter. The Kalman filter model was used for intrusion detection, and its parameters were tuned to improve the model accuracy using the optimizer, by selecting the final R parameter value of the Kalman filter based on the average of R values which performs better for both comprehensive datasets. The system's performance was evaluated using two publicly available intrusion datasets; UNSW-NB15 and CICIDS2017. Results showed that the proposed system achieved an accuracy of 98.801%. for the UNSW-NB15 dataset, and accuracy of 97.02% for the CICIDS2017 dataset respectively.

To further enhance the security of Cyber-Physical Systems (CPSs),[13] proposed a method that integrated "Convolutional Neural Network (CNN) with a Kalman Filter (KF)-based Gaussian Mixture Model (GMM)". A hybrid deep learning model based Siamese Convolutional Neural Network (SCNN) was integrated with Kalman Filtering (HDSCNN-KF) to improve the issue of over-fitting and increase anomaly detection accuracy in CPSs. The GMM was used for data preprocessing. While SCNN analyzed and processed each data to determine whether the data were anomalous or normal. Furthermore, the detected anomalies or threatening activities in CPS were excluded from CPS and normal data was fed into Kalman Filter (KF) that use a failure detector for further analysis and anomaly detection. In that way, KF can analyze and processes the data and identify the anomalies that were missed by SCNN. Results showed detection rate of 98.90% and a false negative rate of 1.10%.

Reference [14] developed an industrial intrusion detection system called "smart security probe" to detect anomaly in a network traffic in other to deduce possible anomalies in the physical process data. Several interlaced extended Kalman filters were introduced into programmable logic controllers for correction and prediction. The system was tested with ARP poisoning and data modification data and results was successful and hopeful.

Reference [15] used a dual axis dimensionality reduction which comprises of "Kalman filter and Salp swarm algorithm" to analyse and minimize data packets. The reduced dataset was then subjected to "a kernel extreme learning machine multiclass classifier for intrusion detection in IoT". The system was evaluated using NSL-KDD, KYOTO 2006+(2015), CICIDS2017 and CICIDS2018 (AWS). Results showed highly reduced data of 70%, 86.43% for the datasets and detection accuracy of between 95.68% and 99.9% with decreased computational time respectively.

The literature reviewed showed that Karman filter can be used for dimensionality reduction, feature selection, artificial neural network weight estimation to enhance the accuracy and detection rate of intrusion detection systems. It can also be combined in three different ways such as Kalman filter with Neural Networks in succession (KFNN), Neural network variables trained by Kalman filter (KFTNN) and Kalman filter variables trained by neural network (NNTKF) [5]. However, NNTKFF models are still in an evolving trend for ameliorating Kalman filter [5]. Moreover, new datasets such as the DoS/DDoS MQTT-IoT which consists of new IoT features needs to be explored [16]. In this research, the Kalman filter was used to estimate the state of the system based on the dataset while the machine learning models were further used to make prediction based on the estimated states. Therefore, it combines KF and ANN, RF, KNN and SVM in the NNTKF manner for attack detection in IoT.

3. METHODOLOGY

3.1. Model Formulation

The hybrid model has two components which work together iteratively to achieve detection.

1. The Kalman filter Estimator

This paper applied a 2D Kalman filter to the dataset as follows:

i. Define the State Transition Model

In this research the state vector is a 2-dimensional vector where each row corresponds to a data sample, and each column corresponds to a feature (or attribute).

a. The initial_state_mean: This is a numpy array representing the initial estimate of the state of the system. we set it to zero in this work, which means it is assume that the initial state is a vector of zeros equal to the number of features. Represented as:

```
initial_state_mean = np.zeros(num_features)
```

b. initial_state_covariance: This is a covariance matrix representing the uncertainty (or error) associated with the initial state estimate. It's a square matrix of size num_features x num_features. The np.eye(num_features) initializes this matrix as an identity matrix, which means there is no initial covariance between state variables. This implies that we assume that the initial state estimate is perfect.

```
initial_state_covariance = np.eye(num_features)
```

c. The transition matrix A is defined as a NumPy array; np.array ([[1]]). This indicates a very simple Kalman filter model where the state is updated by a factor of 1.

The state transition matrix is defined as:

$$x_t = A \cdot x_{t-1} + w \quad (1)$$

Where:
x_t: state vector at time 't'
A: state transition matrix
w: process noise

ii. Observation Model

Each observation has the same number of dimensions as the state vector. The observation matrix H is also NumPy array; np.array ([[1]]). The observation matrix relates the true state of the system to the measurements (observations). It is assumed that the measurements directly correspond to the

true state, and the relationship is linear. This means that the observations are equal to the true state without any scaling or transformation

This is defined as:

$$z_t = H * x_t + v \quad (2)$$

Where:
z_t: the observation at time 't'
H: the observation matrix v: the measurement noise

iii. Filtering Equations
This was implemented using kf.filter(X) as follows:

a. Predicted state estimate
This represents the predicted state estimate at time step t based on the estimate of the previous time step (t-1)
It is represented as:

$$x_t|t-1 = A \cdot x_{t-1}|t-1 \quad (3)$$

Where:

$x_t|t-1$: the predicted state estimate
$x_{t-1}|t-1$: the previous state estimate

b. Predicted Error Covariance
This represents the predicted error covariance matrix at time step t given as:

$$P_t|t-1 = A \cdot P_{t-1}|t-1 \cdot A^T + Q \quad (4)$$

Where:
$P_t|t-1$:the predicted error covariance
$P_{t-1}|t-1$: the previous error covariance
Q: the covariance matrix

transition_covariance (Q): The transition covariance matrix represents the covariance (uncertainty) in the state evolution model. It specifies how the state variables change over time. Here, it's set to an identity matrix, indicating that the state variables are assumed to be independent and have no correlation with their changes from one time step to the next.

c. Kalman gain
This represents the weight applied to the predicted state estimate to calculate the updated state estimate. It is represented as:

$$K_t = P_t|t-1 \cdot H^T \cdot (H \cdot P_t|t-1 \cdot H^T + R)^{-1} \quad (5)$$

Where:
R: the observation noise covariance

observation_covariance (R): The observation covariance matrix represents the uncertainty in the measurements. It indicates how much noise is present in the measurements. Setting it to an identity matrix implies that the measurements are assumed to have no covariance and equal uncertainty for each variable.

d. Updated State Estimate
This represents the updated state estimate at time step t based on the predicted state estimate and the Kalman Gain. It is represented as:

$$x_t|t = x_t|t-1 + K_t \cdot (z_t - H \cdot x_t|t-1) \quad (6)$$

Where:
z_t: the actual observation
$H \cdot x_t|t-1$: the predicted observation weighted by the kalman gain

e. Updated Error Covariance
This represents the updated error covariance matrix at time step t after the update step. It is represented as:

$$P_t|t = (I - K_t \cdot H) \cdot P_t|t-1 \quad (7)$$

2. The Learning Models
four learning models were used in this research. The ANN, RF, KNN and SVM.

The ANN model is a feedforward neural network with three layers: two hidden layers with 64 units each with ReLU activation function and an output layer with a single sigmoid activation unit. The network is used for binary classification (attack or no attack). It also employed a binary cross entropy and an adam optimizer.
The smoothed data obtained from the Kalman filter was used as input for the ANN.

The RF model used a random seed of 50 for the random number generator. this ensures that the results are reproducible when you run the model. In the same vein the SVM model employed a linear kernel (that is kernel ='linear': The kernel function specifies the type of transformation that is applied to the data to find a decision boundary. In this case, a linear kernel was used, which means the model will find a linear decision boundary. The probability=True: This parameter is set to True to enable probability estimates. It allows the model to predict class probabilities in addition to class labels. random_state=42: Similar to the random forest model, setting the random seed ensures that the results are reproducible. While the KNN model parameters were set to default. By default, it used the Euclidean distance to find the nearest neighbors and provided class predictions based on a majority vote from the neighbors.

4. RESULTS AND DISCUSSIONS

For the purpose of this research, the developed hybrid intrusion detection model was tested using the Invalid Subscription flooding sub-data of the DoS/DDoS MQTT-IoT dataset proposed by [16] using ROC-AUC, accuracy, precision, recall and F1 scores as metrics. The dataset was split into training and test set at 75% training set and 25% test set. The ANN training and validation loss vs. epochs showing how the training and validation loss changes over different epochs during the training process is as presented in Figure 1. Also, the training and validation accuracy vs. epochs displaying how the training and validation accuracy changes as the number of epochs increases is as presented in Figure 2. Furthermore, the ROC_AUC, for the hybrid (combination of KF and the

machine learning models) and the individual models without the KF is as shown in Figure 3 and Figure 4. The accuracy, precision, recall and F1score of the hybrid model and the individual models is as shown in Table 1. Figure 5 also shows the accuracy, precision, recall and F1 score of the hybrid model.

In terms of accuracy, Random Forest and ANN models have high accuracy of around 95.7% and 95.5%, respectively, suggesting that they can correctly predict the target variable for most test samples. The SVM model has a slightly lower accuracy 92.3%, indicating it's less accurate in comparison.
In the same vein the F1 scores of Random Forest and ANN models are higher (around 0.9588 and 0.9554, respectively), indicating good balance between precision and recall. Both Random Forest and ANN models also have higher precision (around 0.9832 and 0.9820), indicating that when they predict the positive class, they are highly accurate.
Random Forest model has a recall of around 0.9356, while the ANN has a recall of around 0.9302. These values suggest that they correctly identify a significant portion of the actual positive cases.

The SVM model has a lower accuracy, F1-score, precision, and recall compared to the Random Forest and ANN models. Similarly, the KNN model has slightly lower performance than Random Forest and ANN but is better than SVM in most aspects.

Comparing these results with the results obtained from the stand-alone models. KF enhanced the detection accuracy of the RF, ANN, KNN and SVM by 2.7%, 4.3%, 3.8% and 5.9% respectively. It is important to note that the achieved improvement in accuracy demonstrates the ability of the Kalman filter in enhancing the accuracy of detection models and the model's ability to effectively differentiate between normal network traffic and malicious DoS and DDoS attacks.

Figure 1: ANN Training loss Vs Validation loss

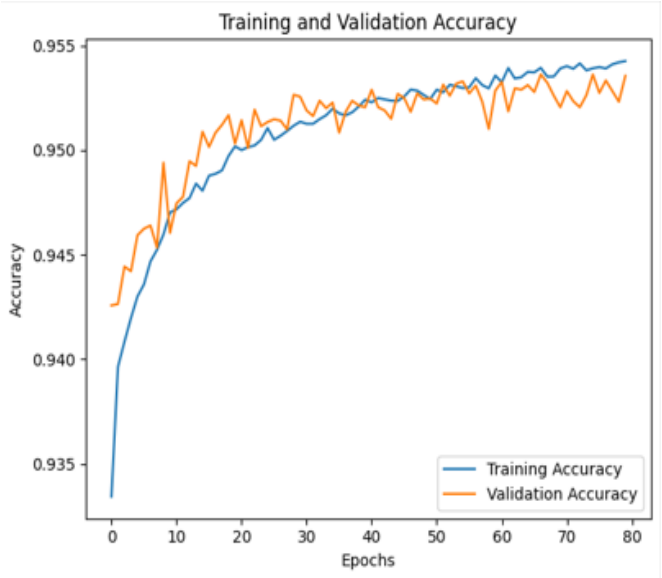

Figure 2: ANN Training Accuracy Vs Validation Accuracy

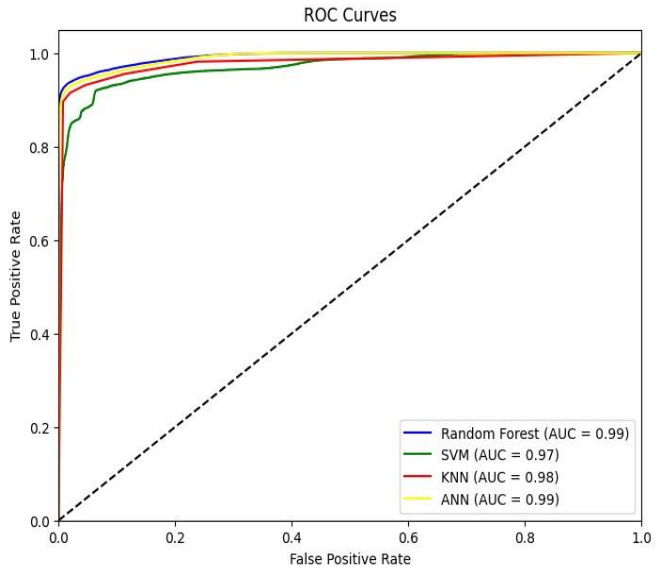

Figure 3: ROC-AUC of the Hybrid Model

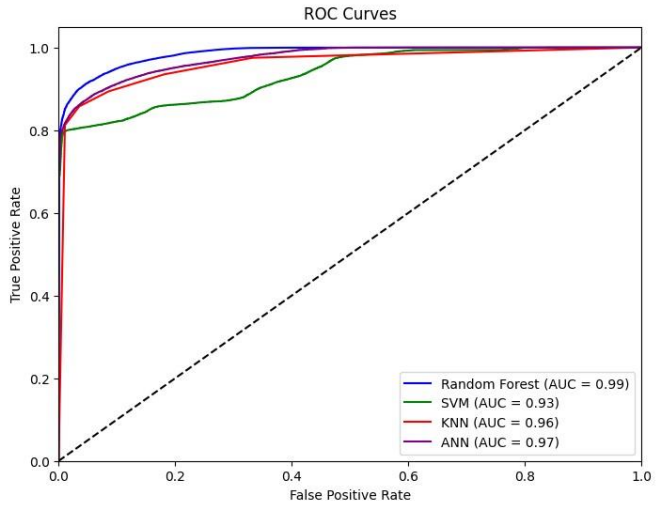

Figure 4: ROC-AUC for the individual Models without KF

Table1: Accuracy, Precision, Recall and F1 scores of the Hybrid vs Individual models

Metrics (%) \ Model	Hybrid Model				Individual Models Without KF			
	KF-RF	KF-ANN	KF-KNN	KF-SVM	RF	ANN	KNN	SVM
Accuracy	95.7	95.5	94.1	92.5	93.0	91.1	90.3	86.4
F1	95.9	95.5	94.4	92.8	93.4	91.4	90.8	86.5
Precision	98.3	98.1	96.0	93.3	93.9	93.9	92.3	92.0
Recall	93.6	93.0	92.8	92.2	93.0	89.0	89.4	81.6

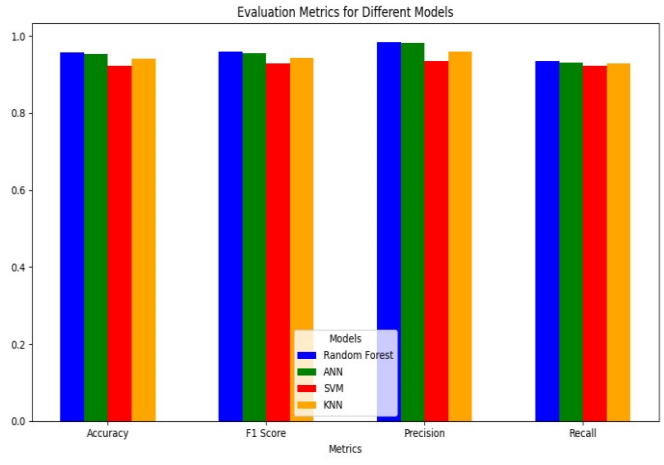

Figure 5: Accuracy, F1-score, Precision and Recall of the Hybrid Model.

5. CONCLUSION

This Research formulated a hybrid model to detect DoS/DDoS attacks in IoT devices. The model combined the estimation capability of Kalman filter with ANN, RF, KNN and SVM Machine learning models. The Kalman filter was used to estimate the state of the system based on the dataset specifically focusing on the Invalid Subscription flooding scenario of the DoS/DDoS MQTT-IoT dataset while the machine learning models were used to make prediction based on the estimated state. The dataset was also simulated using the machine learning models without the Kalman filter. Results showed that the model accuracy, precision, recall and F1 scores were enhanced using the Kalman filter. The hybrid model's performance suggests that the Kalman filter has the potential to enhance the performance of IoT security systems in other to protect against malicious activities. In Future the Kalman Filter parameters will be tuned with optimization algorithm for better performance.

REFERENCES

1. A. A. Diro, and N. Chilamkurti. **Distributed attack detection scheme using deep learning approach for Internet of things.** *Future Generation Computer. Systems.* vol. 82: pp. 761–768, 2018. Doi: 10.1016/j.future.2017.08.043.
2. A.M. Araujo, A. Bergamini de Neira, and M. Nogueira, **Autonomous machine learning for early bot detection in the internet of things,** *Digital Communications and Networks*2022, doi:https://doi.org/10.1016/j.dcan.2022.05.011.
3. N. Ravi and S. M. Shalinie. **Learning-Driven detection and mitigation of DDoS attack in IoT via SDN-Cloud architecture**, in *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3559-3570, April 2020, doi: 10.1109/JIOT.2020.2973176.
4. C. Urrea, and R. Agramonte. **Kalman filter: historical overview and review of its use in robotics 60 years after its creation**, *Journal of Sensors*, vol. 2021, Article ID 9674015, 21 pages, 2021. https://doi.org/10.1155/2021/9674015
5. H. Koyuncu, and B. Koyuncu. **An application of kalman filtering and artificial neural network with k-nn position detection technique.** *Wireless Sensor Network*, vol.9, pp.239-249. 2017 https://doi.org/10.4236/wsn.2017.98013
6. S. Feng, X. Li, S. Zhanga, Z. Jiana,c, H. Duana, and Z. Wang. **A review: state estimation based on hybrid models of kalman filter and neural network**, *Systems, Science & Control Engineering*, vol.11 no. 1, 2173682., pp 1-12, 2023. DOI: 10.1080/21642583.2023.2173682
7. M. Ramasamy, and V. P. Eric. **An improved deep bagging convolutional neural network classifier for efficient intrusion detection system.** *Bulletin of Electrical Engineering and Informatics* Vol. 11, No. 1 pp. 405-413, February 2022. DOI: 10.11591/eei.v11i1.3252
8. S. Chebaane, B. S. Khalifa, F. Hedhili, and S. M. Al-Shomar. **Proposed methods for optical fiber intrusion detection under windy conditions**. *Optik - International Journal for Light and Electron Optics*, vol. 253,168580. 2022 https://doi.org/10.1016/j.ijleo.2022.168580
9. M. Almiani, A. AbuGhazleh, Y. Jararweh, and A. Razaque. **DDoS detection in 5G-enabled IoT networks**

using deep kalman backpropagation neural network. *International Journal of Machine Learning and Cybernetics.* 2021 https://doi.org/10.1007/s13042-021-01323-7

10. J. Liu, W. Zhang, T. Ma, Z. Tang, Y. Xie, W. Gui, and J. P. Niyoyita. **Toward security monitoring of industrial Cyber-Physical systems via hierarchically distributed intrusion detection.** *Expert Systems with Applications*, vol. 158, 2020. 113578. https://doi.org/10.1016/j.eswa.2020.113578
11. S. T. Mohamed, S. Aydin, A. Alkhayyat, and Q. R. Malik. **Kalman and cauchy clustering for anomaly detection based authentication of IoMTs using extreme learning machine.** *IET Communications published by John Wiley & Sons Ltd on behalf of The Institution of Engineering and Technology*. 2022 DOI: 10.1049/cmu2.12467, 1-14.
12. Imran, F. Jamil, and D. Kim. **An ensemble of prediction and learning mechanism for improving accuracy of anomaly detection in network intrusion environments.** *Sustainability* vol. 13 no.18, pp. 1-22. 2021 10057; https://doi.org/10.3390/su131810057
13. M. S. Nagarajan, G. G. Deverajan, K. A. Bashir, P. R. Mahapatra, and S. M. Al-Numay. **IADF-CPS: Intelligent anomaly detection framework towards cyber physical systems**. *Computer Communications* vol.188 pp.81-89. 2022 https://doi.org/10.1016/j.comcom.2022.02.022
14. V. Bonagura, C. Foglietta, S. Panzieri, and F. Pascucci. (2022). **Advanced intrusion detection systems for industrial cyber-physical systems.** in *IFAC-PAPERSONLINE pp.265-270. RADARWEG 29, 1043 NX AMSTERDAM, NETHERLANDS : ELSEVIER [10.1016/j.ifacol.2023.01.083]* 2022
15. S. Gavel, S. A. Raghuvanshi, and S. Tiwari. **Distributed intrusion detection scheme using dual-axis dimensionality reduction for Internet of things (IoT)**. *The Journal of Supercomputing* vol.77,pp. 10488-10511. 2021. https://doi.org/10.1007/s11227-021-03697-5.
16. A. Alatram, L. F. Sikos, M. Johnstone, P. Szewczyk, and J. J. Kang. **DoS/DDoS-MQTT-IoT: A dataset for evaluating intrusions in IoT networks using the MQTT protocol.** *Journal of Network and Computer Applications*, pp 1-8, 2023